Nella Koivisto

Preventing fraud through internal control

Master's Thesis in Accounting

Supervisor: Karolina Söderlund

Faculty of Social Sciences,
Business and Economics

Åbo Akademi University

Turku 2019

Subject: Accounting
Author: Nella Koivisto
Title: Preventing fraud through internal control
Supervisor: Karolina Söderlund

Abstract:

In the past decades, companies have come to a better understanding of the risk of fraud. During the same time, appreciation of internal control has increased. The degree of internal control varies, however, between companies. Even though previous research has indicated that internal control offers a tool for fraud prevention, studies have shown that there are companies that use ineffective controls.

The objective of this thesis was to increase the understanding of how companies use internal control to minimise the risk of internal fraud in a European context. In addition, effectiveness of different types of controls was researched; areas for improvement were also considered. Semi-structured interviews were used as the research method. Both internal and external stakeholders were interviewed to obtain a broader understanding of the topic.

The results show that the level of internal control and the types of controls vary based on a company's size, industry and level of risk. Some basic controls, such as access rights controls and segregation of duties, are, however, found in almost all companies. Automated and built-in controls combined with the right company culture and 'tone at the top' were considered the most effective controls. Ignorance and overreliance on ineffective controls and on certain individuals were considered factors that weaken internal control. The results indicate that adaptation of the internal control to each company as well as regular monitoring and assessment of the controls could improve internal control.

Keywords: Internal fraud, occupational fraud, internal control, fraud triangle, COSO framework

Date: 15/12/2019	**Number of pages:** 64

Table of Contents

List of abbreviations

ACFE - Association of Certified Fraud Examiners

CoCo – Criteria of Control framework

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CPI – Corruption Perceptions Index

FERF – Financial Executives Research Foundation

EU – European Union

IAASB – International Auditing and Assurance Standards Board

IIA – Institute of Internal Auditors

IPPF – International Professional Practices Framework

SEC – U.S. Securities and Exchange Commission

SOX – Sarbanes-Oxley Act

USA – United States of America

1 Introduction

Fraud prevention has received increased attention in companies in the past decades. Especially after fraud scandals, such as the Enron scandal in 2001, the risk of fraud has been better acknowledged in companies. According to Arwinge, Eklöv Alander and Nilsson (2013), development of internal control has received attention worldwide in past years. Pickett (2012) argues that besides the increased understanding, companies are also facing an increased threat of fraud. According to Pickett, the narrowing hierarchy and transience of the modern workplace have led to an expanded risk of fraud.

The concept of fraud can be divided into three types: internal fraud, also called occupational fraud, external fraud and fraud against individuals. Internal fraud can be further divided into corruption, asset misappropriation and financial statement fraud. Fraud poses a significant risk for companies. According to the Association of Certified Fraud Examiners' (ACFE, 2018a) "Report to the Nations 2018: Global Study on Occupational Fraud and Abuse", organisations lose in median 5 per cent of their annual revenues to fraud (ACFE, 2018a). Accountancy Europe (2019) also highlight that, according to the Grand Theft Europe project, annually 50 billion euros is embezzled in the tax context, in the area of the European Union (EU) Member States, Norway and Switzerland. Pickett (2012) underlines the severity of fraud and states that even criminal actions, such as human trafficking, have been financed with fraudulent funds. Out of the three types of internal fraud mentioned above, asset misappropriation is the most common within companies (ACFE, 2018a). Financial statement fraud, in turn, causes the greatest losses for the victim companies (ACFE, 2018a). In addition, Dimitrijevic, Milovanovic and Stancic (2015) argue that financial statement fraud decreases the public's trust in audit opinions as well as trust in the quality of financial reporting and may thus even deteriorate the accountancy profession's image. In addition to the types of fraud, different theories aim to explain why people commit fraud; the fraud triangle is an example of these theories. The fraud triangle theory is explained in detail in chapter two.

The appreciation of internal control has increased in recent years. Ahokas (2012) mentions that internal control can generally be defined as measures and actions which control a company's operations. The execution of internal control is not regulated in Europe. There are several variations of internal control definitions and companies use it in divergent ways to various purposes. There are, however, frameworks which guide and facilitate the implementation of internal control procedures. The COSO framework was introduced in 1992 and is the most cited framework in the field (Ahokas 2012; Wikland, 2014; Arwinge et al., 2013; Marshall, Isaac and Ryan, 2006). According to COSO (1994), the five components of effective internal control are: control environment, risk assessment, control activities, information and communication, and monitoring. There has been a movement to set legal requirements for internal control. For example, in the United States of America (USA) the Sarbanes-Oxley Act (SOX) took effect in 2002 (Wikland, 2014). SOX regulates the quality of internal control related to financial statements (Wikland, 2014). Internal control procedures offer a possibility to assess and monitor the risk of fraud. Furthermore, there has been increased interest in the field of research to examine the relationship between fraud and internal control and the effectiveness of internal control as a fraud prevention tool.

1.1 Research context

Internal control is implemented and used in different ways in companies. In addition, there has been discussion about the effectiveness of internal control as a fraud prevention tool. On the one hand, several studies mention that internal control is an effective tool in preventing and detecting fraud (Petersen, Bruwer and Le Roux, 2018; Puspasari and Suwardi, 2016; Mirinaviciene, 2014; Shanmugam, Haat and Ali, 2012; Barra, 2010; Rae and Subramaniam, 2008). On the other hand, studies indicate that companies tend to use ineffective internal control measures (Nawawi and Salin, 2018; Petersen et al., 2018; Zakaria, Nawawi and Salin, 2016). According to Donelson, Ege and McInnis (2017), the relationship between internal control and fraud lacks empirical evidence. Their study offers needed empirical evidence which indicates that weaknesses in internal control procedures are red flags for possible future fraud within the company. Furthermore, Westhausen (2017) notes that internal audit's role as an anti-fraud tool has increased.

1.2 Objectives of the research

As mentioned above, even though studies indicate that internal control offers a tool for fraud prevention, there is a risk that companies use ineffective controls. The objective of this thesis is to increase understanding of how companies use internal control to minimise the risk of internal fraud in a European context. The aspect of ineffective internal controls will be addressed with questions related to effectiveness of the different types of controls. The level of internal control will be examined with interviews with people in different positions both inside and outside different organisations. The research questions will thus be:

1. *How do companies use internal control to prevent internal fraud?*
2. *Which types of controls are considered the most effective for internal fraud prevention?*
3. *What are the areas for improvement in preventing internal fraud through internal control?*

It is important to evaluate the current level of internal control procedures related to fraud prevention in order to identify possible insufficiencies. What is more, the study indicates possible strengths and weaknesses in fraud prevention procedures within companies. The results also contribute to identifying the most efficient internal controls for fraud prevention.

1.3 Structure

In the next section of the thesis, in chapter two, theory concerning fraud is explored, while the theory related to internal control is examined in chapter three. In the fourth chapter, the aspect of risk management is presented. In the fifth chapter, previous studies are analysed. Thereafter, in the sixth chapter, the research method, sample and the strategy for analysing the collected data are explained. Then in the following, seventh chapter the results of the interviews are presented. In the eighth chapter, the results of the interviews are analysed and discussed in relation to the research questions, theory and results from

previous studies. Finally, in the ninth and the final chapter, the conclusions of the research and suggestions for future research are discussed.

2 Fraud

In this chapter, the concept of fraud and related theories are discussed in detail. In the beginning of this chapter, several definitions of fraud are presented. After this, the different categories of fraud are described. Finally, at the end of this chapter, seven theories related to fraud are presented.

Fraud can be defined in different ways. Accountancy Europe (2017) note that there is no uniform international definition of fraud. According to Accountancy Europe, financial crime is an umbrella term for varied crimes, such as fraud and corruption, whereas ACFE (2018a), for instance, classify corruption as a subcategory under fraud.

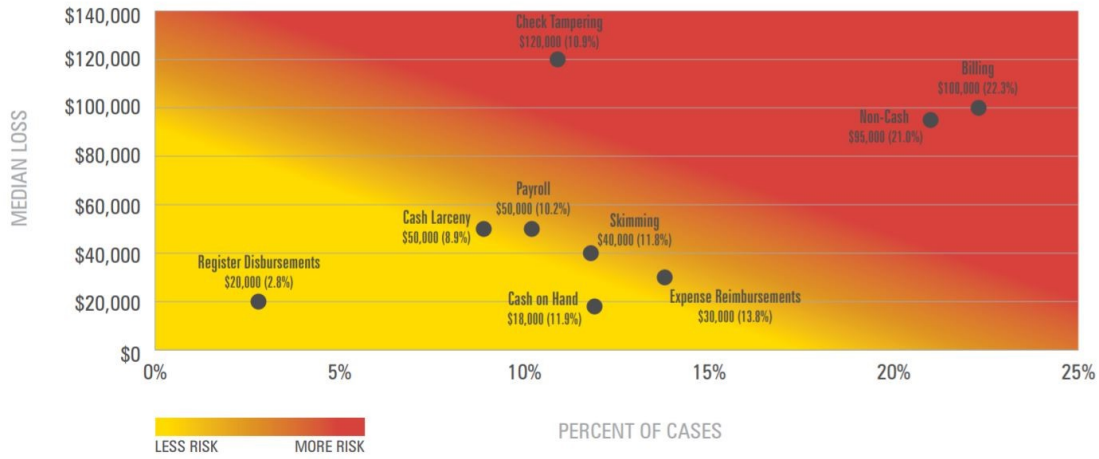
According to Biegelman and Bartow (2012, pp. 24), in Black's Law Dictionary fraud is defined as "the knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment and a misrepresentation made recklessly without belief in its truth to induce another fact." World bank (2014, pp. 3) define fraud as "any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation." Accountancy Europe (2017) remark that the International Auditing and Assurance Standards Board's (IAASB) definition covers only internal fraud categories financial reporting and misappropriation of assets, which are explained more in depth later in this chapter. IAASB (2016, pp. 23) define fraud as "an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage." Furthermore, Transparency International (2019a) define fraud as "the offence of intentionally deceiving someone in order to gain an unfair or illegal advantage (financial, political or otherwise)."

2.1 Internal and external fraud

According to ACFE (2018b), fraud can be divided into internal fraud, external fraud and fraud against individuals. In this thesis, only fraud against companies is studied. Pickett (2012) lists that the four main targets of fraudsters are data, assets, expenditure and income. Moreover, ACFE (2018a) state that internal fraud can be committed by all internal actors, that is, employees, managers and owners of the company. ACFE define internal fraud, also called occupational fraud, as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplications of the employing organization's resources or assets." (ACFE, 2018a, pp. 6). According to ACFE, internal fraud can be divided into subcategories: asset misappropriation, corruption and financial statement fraud. External fraud, on the other hand, can be committed by customers, vendors or other parties (ACFE, 2018b). According to ACFE, external fraud covers, for instance, dishonest customers using forged payment information or dishonest vendors invoicing undelivered goods. In addition, other parties may commit, for example, a tax or a loan fraud. This thesis focuses solely on internal fraud as defined by ACFE (2018a).

According to ACFE's (2018a) Report to the Nations, asset misappropriation is the most common type of internal fraud. ACFE (2018a) describe asset misappropriation as theft or misuse of employer's resources. The asset misappropriation frauds can be further divided into cash and non-cash asset schemes. According to ACFE, for example, theft of company cash and fiddling the expense reports represent asset misappropriation within companies. Despite being the most common type of internal fraud, asset misappropriation causes the lowest median loss, USD 114,000, for a victim company. Moreover, ACFE (2014) describe that asset misappropriation consists of nine sub-categories of which check tampering, billing and non-cash schemes imply the greatest risk for a company. The nine sub-categories and the risks they comprise are visualised in Graphic 1.

Graphic 1: Frequency and median loss of asset misappropriation sub-categories



Reference: ACFE Report to the Nations on occupational fraud and abuse (2014, pp. 13)

According to ACFE's (2018a) Report to the Nations, corruption is the second most common type of internal fraud. ACFE (2018a) define corruption as a scheme in which an employee tries to gain direct or indirect advantage by exploiting his impact in a business transaction. Moreover, the behaviour neglects the employee's duty to the employing organisation. ACFE name that bribery, conflict of interest, illegal gratuities and economic extortion schemes are the main categories of corruption. ACFE (2018a) mention that organisations which were victims of corruption suffered a median loss of USD 250,000. Transparency International (2019b) mention that Denmark, Finland, Sweden and Switzerland are the top scoring countries in the annual Corruption Perceptions Index (CPI), while Bulgaria, Greece and Hungary scored the lowest. They stress, however, that corruption is present even in the top CPI countries. According to Transparency International, although a country's public sector indicates low corruption, it still occurs. They illustrate the risk with an example of money laundering scandal in Denmark within the banking sector. In addition, for example in Finland, a football club chairman was committed of fraud in spring 2019 (Vähämäki, 2019). Transparency International (2019b) argue that therefore, also in countries with low corruption according to the CPI score, proactive measures are required. According to Transparency International (2019c), corruption causes economic, political, social and environmental costs. Transparency International describe that, from the economical perspective, corruption can channel resources into undesirable destinations instead of urgent projects. In addition,

Transparency International explain that corruption creates obstacles for fair market processes and competition.

The third type of internal fraud is financial statement fraud. ACFE (2018a) characterise financial statement fraud as an employee's intentional misconduct through which he falsifies the employing organisation's financial statements. According to ACFE, the misconduct can, in particular, appear as misrepresentation or omission of material information in the financial reports. ACFE describes that the two main groups of financial statement fraud are net income over- and understatements. For instance, registering fabricated revenues and artificially augmenting reported assets are, according to ACFE, examples of financial statement fraud. ACFE's Report to the Nations 2018 signals that whilst financial statement fraud is the rarest type of internal fraud, it causes the greatest loss to the victim companies, a median loss of USD 800,000. Biegelman and Bartow (2012) note that while recovery from asset misappropriation is often attainable, financial statement fraud can be destructive for an organisation.

2.1 Fraud triangle

Biegelman and Bartow (2012) mention that the fraud triangle was developed and first introduced by Dr. Donald Cressey. The aim of the theory is to explain why fraud is committed. Biegelman and Bartow describe that, according to Dr. Cressey, the three components that lead to fraud are motive, rationalisation and opportunity. The relationship between the three components is visualised in graphic 2. Biegelman and Bartow underline that the components are linked and that they must exist simultaneously. Moreover, if even one of the components is missing fraud is avoided.

Graphic 2 The fraud triangle

Reference: Biegelman and Bartow (2012, pp. 32)

The first element in the fraud triangle is financial pressure - or more generally motive. Biegelman and Bartow (2012) discuss that financial pressure is a common reason to commit fraud. The motive can, however, be a different one as well. Biegelman and Bartow describe that motive is the factor which drives a person to break the law. They mention that greed is often a common factor for the different motives. According to Biegelman and Bartow, for instance, debt or gambling addictions are examples of possible motives to commit fraud. Furthermore, Biegelman and Bartow remark that even revenge or ego can prompt a person to commit fraud. They mention that also pressure within company to generate results can lead a person to embellish results.

The second element in the triangle is opportunity. According to Biegelman and Bartow (2012) opportunity is defined by how easy it is to commit fraud. Dimitrijevic et al. (2015) highlight the importance of the opportunity element. They reason that for fraud to happen the fraudster must identify a way to commit it. Biegelman and Bartow (2012) describe that the possibility to commit fraud is often affected by the person's position in the company, that is, the amount of authority, or the level of access to resources. They argue that the opportunity element of the fraud triangle can be limited with internal control. Biegelman and Bartow mention that ineffective internal control provides an opportunity to commit fraud. They emphasise that opportunity is the element which companies can

best control in order to prevent fraud. Thus, it is essential that companies minimise the opportunity to commit fraud within the company.

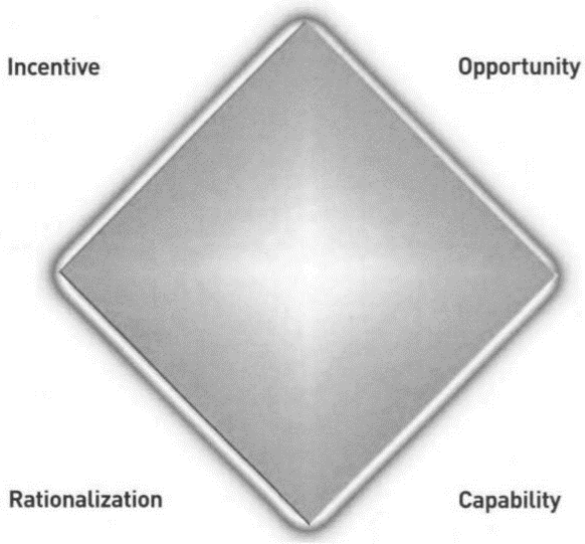
Finally, the third element of the triangle is rationalisation. Biegelman and Bartow (2012) describe that the rationalisation represents justification of an action. They explain that the fraudster explains to himself through rationalisation why it is acceptable to break the law or in another way act inappropriately. Biegelman and Bartow remark that fraudsters tend to believe that unsuitable behaviour is acceptable when the elements of both motive and opportunity occur. Furthermore, Biegelman and Bartow note that the fraudsters often view themselves as victims and justify the actions through different rationalisations, such as “They owe it to me” or “Everybody does it” (Biegelman and Bartow, 2012, pp. 35). Biegelman and Bartow mention that rationalisation prevents conscious from taking control. Childers (2009) argues that recession tends to strengthen the presence of the above-mentioned elements: motive, opportunity and rationalisation. He specifies that, even though the opportunity element is the easiest to control, it is vulnerable to manipulation and misconduct.

Biegelman and Bartow (2012) note that the fraud triangle has also been criticised. They mention that Dr. Steve Albrecht found in his studies that some conditions, such as pressure to have status or a lifestyle which exceeds the means, were more likely to lead to committing fraud. Biegelman and Bartow describe that, in line with Cressey’s fraud triangle, Albrecht argued that even if both motive and opportunity existed some people would sustain from committing fraud. Biegelman and Bartow remark, however, that Albrecht criticised the simplicity of the fraud triangle. They mention that he suggested that the three elements of the fraud triangle are more complex. Biegelman and Bartow describe that, according to Albrecht, the elements of fraud triangle exist on different levels depending on the situation. According to Biegelman and Bartow, Albrecht suggests that the extent of motivation to commit fraud could be understood by a Fraud scale which defines the strength of the different elements of the fraud triangle.

2.2 Fraud diamond

Since its introduction in the seventies, the fraud triangle has been further developed. The fraud diamond, for instance, is a variation of the original triangle. Biegelman and Bartow (2012) describe that the fraud diamond expands the original model by adding a fourth element, capability. The fraud diamond is visualised in graphic 3.

Graphic 3 The fraud diamond



Reference: Wolfe and Hermanson (2004, pp. 38)

Biegelman and Bartow (2012) mention that the capability represents personality and traits. They argue that factors such as intelligence, creativity and self-confidence are essential because the employee must identify possible situations to commit fraud but also cope with the stress related to it. Moreover, Wolfe and Hermanson (2004) mention that capability is the element which ultimately enables the fraud. They highlight the following six factors of which capability consists of: position within the company, intelligence, ego, ability to persuade, ability to lie and stress tolerance. Wolfe and Hermanson suggest that monitoring employees' capabilities to commit fraud is an essential part of preventing and detecting fraud within companies. In fact, they mention that little things, such as refusal to lose, can indicate capability to fraudulent behaviour. They remark that, for instance, cheating in golf can be a warning sign of capability to commit fraud.

2.3 Other fraud theories

Similar to the fraud diamond described earlier in this chapter, Pickett (2012) also describes that, according to the Fraud smart model, four factors cause the threat of fraud. He argues that the four elements are benefit, access, motive and concealment. With benefit Pickett refers to any type of advantage, such as financial gain or even revenge. Access element is similar to the opportunity in the fraud triangle and diamond. Pickett describes access as possibility to reach the benefit the person tries to obtain. He notes that the access element is harder to limit if the fraudster is from within the company. The motive element is also comparable to the fraud triangle's motive element. In the Fraud smart model, the motive represents the need for something, such as money. Pickett (2012, pp. 142) describes that the fourth element, concealment, refers to "the art of not getting caught". Concealment thus corresponds to the capability element of fraud diamond. Overall, the Fraud smart model is very similar to the previously described fraud triangle and diamond. The Fraud smart model differentiates, however, of the two models with the benefit element and slightly different grouping of the other elements.

In addition to the theories described above, Biegelman and Bartow (2012) introduce several other theories they have developed. The "Tip of the Iceberg Theory" refers to the fact that often during the investigation process frauds are found to be larger than first suspected. The "Potato Chip Theory" is another theory Biegelman and Bartow introduce. According to this theory, fraudsters tend to commit fraud again. Biegelman and Bartow argue that fraud can become a type of addiction, which leads to the fraudster committing new frauds and taking bigger risks. A third theory described by Biegelman and Bartow is called the "Rotten Apple Theory". This theory refers to the phenomenon where employees become fraudulent when they notice someone else commits fraud without consequences. Biegelman and Bartow explain that the "Low-Hanging Fruit Theory" in turn, assumes that fraudsters will seek for the easier targets since there are less controls and thus less risk of being exposed. Therefore, Biegelman and Bartow reason that even the lower risk frauds should be addressed.

3 Internal control

In this chapter, internal control is presented more in detail. In the beginning of this chapter the definition of internal control is discussed further. Thereafter, the concept of internal audit is described. Then the COSO framework is presented in detail. Finally, the challenges and limitations of internal control are discussed in the end of the chapter.

There is no one correct way to define internal control. Different companies can use different internal control functions for different purposes. Internal control can generally be defined as measures and practices that control a company's operations (Ahokas, 2012). Arwinge et al. (2013) note that the concept of internal control was introduced over 100 years ago, while the internal control procedures' significance has in the past decades increased. Brown (1962) argues that the first recognitions of internal control appeared in 1905. This was due to Lawrence Dicksee's (1905) publication "Auditing" on audit duties and practices. Maijoor (2000) describes that internal control was earlier often defined as accounting controls. He notes that the definition has later broadened and nowadays a more extensive definition is used. According to Dimitrijevic et al. (2015), in the beginning internal control's role in the fraud context was focused on fraud detection. They mention that with the development of the scope of internal control also the focus within the fraud context has shifted towards fraud prevention.

The COSO framework represents the wider definition of internal control. The COSO framework is discussed more in detail later in this chapter. According to Spira and Page (2003) the Criteria of Control Framework (CoCo), developed by Canadian Institute of Chartered Accountants, is another framework that represents the wider definition of internal control. This thesis focuses on the COSO framework as it is the most cited internal control framework (Ahokas 2012; Wikland, 2014; Arwinge et al., 2013; Marshall et al., 2006). Ahokas (2012) describes that internal control is used to ensure that a company functions according to its goals and instructions. She explains that internal control procedures aim to prevent and detect flaws, mistakes and malpractice. Arwinge et al. (2013) argue that internal control procedures should be integrated to other management functions. They describe that in case internal control is unintegrated with

the other management functions, the internal control procedures might, for instance, lack updates when new strategies are introduced. Ahokas (2012) emphasises that the effectiveness of internal control is more important than the way it is arranged. According to Ahokas, internal control is effective when it secures the management and board of directors that the financial information is reliable and that possible weaknesses would be detected. She also remarks that the costs of internal control should be reasonable compared with the gained benefit. In general, companies can choose how to implement internal control. However, the COSO framework provides a general model for internal control. Furthermore, in the USA the use of internal control is regulated by the Sarbanes-Oxley Act. The COSO framework and Sarbanes-Oxley Act are described more in depth later in this chapter.

3.1 Internal audit

Ahokas (2012) mentions that internal audit is often confused with internal control. Internal audit is, however, only a part of internal control. Ahokas defines internal audit as an independent and objective organisation. In addition, she explains that internal audit procedures are guided by the International Professional Practices Framework (IPPF), published by the Institute of Internal Auditors (IIA). IPPF defines, for example, ethical and practical guidelines for internal audit (Ahokas, 2012). According to Ahokas, the internal audit function is often a separate unit, whereas internal control is integrated in the whole organisation. The management is the main responsible for internal control. Dimitrijevic et al. (2015) underline the internal audit's role in assessing and ensuring the quality of internal control in companies. They argue that when a company lacks internal audit it is crucial that more of the other control measures are used to ensure an effective internal control system.

3.2 COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) introduced a framework for internal control in 1992. Arwinge et al. (2013) describe that

the COSO framework was an outcome of stakeholders' requirements. They specify that shareholders and other stakeholders stipulated more effective control to prevent fraud within companies. According to Marshall et al. (2006), the COSO framework is the most used internal control framework in companies that are affected by the Sarbanes Oxley Act. COSO (1994) define internal control as a process, which offers reasonable assurance that objectives are obtained in the three following categories: "effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations" (COSO, 1994, pp. 3). According to COSO (1994), effectiveness and efficiency of operations refers to business goals, such as targets for profitability and performance. Regarding reliability of financial statements, the framework addresses preparing financial statements and other reports in a reliable manner. Finally, in the third category, the laws and regulations related to the organisation are handled. The internal control process is executed within the company by management, board of directors and other personnel (COSO, 1994).

The COSO framework divides internal control into the following five parts: control environment, risk assessment, control activities, information and communication, and monitoring (COSO, 1994). COSO (1994) describe that these five parts are linked and together create a system which reacts to changes in conditions. Furthermore, COSO argue that the framework's five components are linked to the three earlier mentioned categories. According to COSO, the three categories represent what an organisation aims to accomplish, while the five components explain what is required to accomplish this.

3.2.1 Control Environment

COSO (1994) describe how the control environment creates the ground for the four other parts of internal control. COSO explain that it offers structure and control but also influences the control consciousness within the organisation. According to COSO, the control environment covers, for example, integrity, ethical values, way of distributing responsibility or authority, and how people are organised and developed. Marshall et al. (2006) summarise that the control environment part of the COSO framework establishes a base for internal control as it defines the control awareness within a company. The

control environment includes seven factors. COSO (1994) remark that depending on the type and the size of the organisation the needed broadness of the different factors varies.

The first factor is integrity and ethical values (COSO, 1994). COSO note that management's integrity and how committed they are to ethical values is reflected on organisation's objectives and the way they are achieved. Furthermore, COSO argue that integrity and ethical values affect the quality of the four other parts of internal control. According to COSO, top management has a significant role in communicating a company's ethical values and appreciated behaviour. COSO add that the top management can communicate the values through a code of conduct. According to Transparency International (2019a), code of conduct outlines rules for behaviour within a company. Moreover, Transparency International describe that the code of conduct specifies the minimal requirements concerning compliance and disciplinary actions. Pickett (2012) underscores that the code of conduct should be simple and clear enough so that everyone within the organisation understands it. COSO (1994) note, however, that the management's behaviour and actions are equally important, since the employees tend to follow the example set by management. Sinnett (2009) mentions, however, in his article "Does Internal Control Improve Operations and Prevent Fraud?" that for example Roland Laing, a retired Financial Executives Research Foundation (FERF) president, has commented that the crises in the economy in the years after the release of the framework could be seen as signals of management's difficulties in setting the tone.

The second factor is commitment to competence (COSO, 1994). According to the COSO framework, an employee's task should be connected to his level of competence. COSO also mention that the required competence level depends on management's decision on how well the tasks should be done. In addition, COSO explain that the costs should be considered because high competence employees are more expensive while low competence employees often require more supervision.

The third factor is board of directors and audit committee (COSO, 1994). According to the COSO framework, factors regarding the board of directors which affect the control

environment are, for instance, its independence from the management, experience and importance. Moreover, COSO describes that the board of directors should challenge the management and ask difficult questions regarding the top management's activities. Hence, COSO argues that, to ensure the board's effectiveness, the board of directors should include even outsider directors.

The fourth factor is management's philosophy and operating style (COSO, 1994). According to COSO, it addresses, for example, accepted business risk but also attitudes towards financial reporting and choice of accounting principles. The next, that is the fifth, factor is organisational structure. The COSO framework emphasise that the appropriate structure depends on the nature and size of the organisation. COSO explains that the structure should, however, create pertinent lines of reporting and specify the key areas of responsibilities and authority.

The sixth factor is assignment of authority and responsibilities (COSO, 1994). COSO argue that authority and responsibilities should be assigned to operating activities. In addition, COSO note that the allowed level of initiative and limits of authority should be defined. The framework underlines that every employee should understand his actions effect on the achievement of objects. Pickett (2012) also emphasises that what is expected of the employees must be clear. He adds that organisations should offer training to enable the employees to fulfil the expectations. Another remark by COSO (1994) is that the recognised level of accountability affects the organisation's control environment. Finally, the seventh factor is human resource policies and practices. COSO mention that, for example, hiring and training practices signal the expected ethical behaviour and competence to the employees.

COSO (1994) emphasise that control environments between companies differ mostly due to different managerial styles. The framework underlines the importance of understanding that the differences in control environment also affect the four other internal control components. Furthermore, COSO accentuate that small and mid-size organisations should adapt the framework to their needs since a large organisation is likely to require

more formal control. Another remark by the framework is that when evaluating the control environment each of the above mentioned seven factors should be examined. Childers (2009) argue that conversations between managers and employees can reveal weaknesses in the control environment. He argues that, therefore, information from these discussions can be valuable input for the evaluation. Childers concludes that with a general database for a company, for example, an internal auditor can identify larger weaknesses and suggest improvements to the internal control procedures. Marshall et al. (2006) note that in 2004 COSO revised parts of the internal control framework. The control environment section was divided into internal environment and objective setting to provide a clearer picture of the component.

3.2.2 Risk Assessment

COSO (1994) remark that an organisation's objectives must be defined before assessing the risks. COSO explain that once the objectives are defined the organisation can determine the risks related to them and how the risks should be managed. COSO add that even risks caused by potential changes in the company's surroundings, for example in economy and industry, must be identified and analysed.

As mentioned above, a company must define its objectives before it can analyse and control the risks. COSO (1994) remind that even though objective setting is not a component in the framework, it is a precondition to the process. According to the COSO framework, the objectives are a part of a company's strategic plan. COSO explain that there are various ways to determine the objectives; the process can be either structured or informal. COSO add that both implicit and explicit objectives are possible. The COSO framework describes that more detailed objectives are called subobjectives. According to COSO, these subobjectives relate to different activities within the company. Identification of the company's critical success factors is possible once the objectives are clear. COSO describe that the critical success factors are elements and activities which are essential in obtaining the objectives. There is a variety of possible objectives. The COSO framework identifies, nevertheless, three main categories. The first category is operations objectives. According to COSO, these objectives are related to effectiveness and efficiency. COSO

explain that, for example, strategic decisions and the core business affect these objectives and they can vary broadly between companies and fields. The second category is financial reporting objectives. According to COSO, these goals are strongly related to external requirements and they aim to secure reliable financial statements. The third category is compliance objectives. COSO describe that, similar to the second category, also these objectives are related to external requirements. COSO explain that these goals relate to complying with laws and regulations. COSO remind that there is, nonetheless, overlap between the three categories and circumstances can affect the categorisation.

All companies encounter risks in their operations. Although the risks should be mitigated, COSO (1994) remind that a zero level of risk is impossible to obtain. Therefore, the framework argues that companies must decide the accepted level of risk. The COSO framework argues that risk identification and examination is a crucial part of internal control and they must be managed on all levels of the organisation. The framework describes that both external and internal factors can pose risks to a company's operations. Change in operations increases the company's risks and COSO framework notes that companies with new objectives have larger risks. Nonetheless, COSO note that even companies pursuing similar performance as previous years encounter risks due to, for example, changes in the market. COSO argue that in the risk identification process companies should acknowledge all important and critical activities and interactions.

COSO (1994) describe that, for instance, technological developments, new legislation and customer needs are external factors which create risks for companies. COSO mention that unconvincing board of directors, employee accessibility to assets and quality of personnel are examples of risk creating internal factors. COSO framework describes that high-risk activities can be identified with quantitative and qualitative methods. According to COSO, even industry reviews and management conferences offer possibilities to identify risks. The COSO framework remarks, however, that instead of the chosen methods the identification process' fundamental part is to consider all the risk generating factors. COSO describe that finally, the importance of these factors must be determined. COSO argue that, besides assessing risks on entity level, they should also be assessed on

activity level. The COSO framework mentions that this enables identifying risks in large departments, such as sales and production.

Once the risks are identified, they must be analysed. According to COSO (1994), the analysis process consists of evaluating the significance and the likelihood of the risk. In addition, COSO explain that the activities related to managing the risks are considered. COSO note that only the significant risks which are likely to occur should receive a great amount of attention. COSO framework remarks, however, that it is often difficult to outline the risks that a company should focus on. According to the framework, the size of a risk can be large, moderate or small. Risk management is discussed more in depth in chapter four.

COSO (1994) describe that change in conditions within a company, such as new personnel or new information systems, also pose risks for companies. COSO argue that companies must have processes which identify the risks caused by change. It is essential to have early warning systems which will alert the company of possible future risks. As mentioned earlier in this chapter, the framework was revised in 2004. Marshall et al. (2006) describe that in the 2004 update the risk assessment section was divided into event identification, risk assessment and risk response.

3.2.3 Control Activities

According to COSO (1994), the actions and policies which secure the realisation of management's directives in a company are called control activities. COSO describe that the control activities include different actions, such as authorisations and segregation of duties, and they exist throughout the company structure. Marshall et al. (2006) underline that anomalies in processes are identified or prevented with control activities. This way the controls assure that processes function in an intended manner.

COSO (1994) describe that there are three categories of control activities. The categories are operations, financial reporting and compliance. However, COSO explain that the

categories overlap, and some activities belong to several categories. COSO add that there are also various types of controls, such as preventive and detective controls. The COSO framework mentions that top level reviews, that is, comparing the materialised performance with, for example, budget or previous years, and segregation of duties, that is, separating authorities for closely related duties, are examples of possible control activities.

COSO (1994) state that there are two elements in control activities. First, a policy defines what is required. COSO emphasise that policies should be clear and executed consistently and thoroughly. Second, procedures ensure that policies are fulfilled. COSO explain that procedures control different elements of policies, such as the nature of the traded securities. In addition, COSO argue that the effectivity of the procedures should be controlled regularly.

COSO (1994) underline that companies must link the control activities to the earlier discussed risk assessment component. COSO add that the risk assessment process enables also the identification of correct control activities. Moreover, COSO note that the controls must support the achievement of the company's objectives. According to COSO, the control activities offer a possibility to examine the company's performance and progress.

COSO (1994) describe that due to the wide use of information systems in companies, various controls for these systems are required. COSO explain that the control activities over information systems can be general controls, which apply to all information systems. COSO mention that, for instance, access security controls are examples of general controls. COSO add that application controls are another type of information system control. They apply to specific information systems. The COSO framework underlines that the two types of controls are linked. COSO argue that right and functioning general controls are needed to ensure the effectiveness of the application controls.

COSO (1994) remark that all entities have entity specific controls. COSO describe that different entities have different controls due to, for example, differences in fields and

people who work in the entity. The framework also rationalises that more complex entities will require more control activities, while simpler entities manage with fewer controls. COSO framework reminds that companies should always adapt the control activities to company, entity specific objectives and other factors.

3.2.4 Information and Communication

COSO (1994) emphasise that gathering and communicating information should be conducted in a way that allows normal performance on other tasks. COSO explain that the gathered information is thereafter transformed into reports by information systems. According to COSO, these reports offer information about both internal and external circumstances. Moreover, the COSO framework stresses the importance of an efficient information flow which functions across the organisation. COSO argue that the top management should explicitly communicate the importance of the control activities, while also the employees should have a possibility to communicate significant information upstream.

COSO (1994) underscore that companies must only collect relevant information and it must be communicated to the right people. COSO describe that the gathered information supports a company's decision-making processes. The COSO framework mentions that financial information, for instance, is used in operating decisions, while operating information is required to build the financial statements. COSO describe that information systems are used to handle the data. COSO explain that the information systems are involved in all the processes related to information, that is, identifying, collecting, processing and reporting the information. COSO note that information systems enable better control over activities. The COSO framework demonstrates this with an example of an insurance company which can easier follow how many payments have been made in a period when the information is in an information system, rather than on paper. More generally, COSO describe that information systems enable management and personnel to better follow various activities within a company and detect possible anomalies. In addition, COSO argue that the quality of the information must be verified by checking

that the required information exists and that the information is timely, current, accurate and accessible.

As mentioned above, information must be communicated to the right people. Moreover, information is communicated both internally and externally. COSO (1994) underline that besides the information related to operations, also the importance of internal control procedures must be explicitly communicated by the management. Moreover, COSO add that personnel's specific responsibilities and activities must be clearly communicated. In addition, COSO note that the management must clarify that reasons for any anomalies must be examined. Equally important, COSO remind that the employees must have a possibility to communicate information upstream. COSO remark that for the communication channel to function, the top management must indicate that they will listen. According to COSO, communication between the top management and the board of directors must also function effectively. COSO remark that companies must even have effective communication with external parties. COSO argue that external parties, such as customers, can offer important information to companies. What is more, COSO describe that companies must communicate also to the external parties that misconduct or illegal actions are not acceptable.

3.2.5 Monitoring

COSO (1994) describe that the effectiveness of the internal control systems must be overseen through monitoring activities and separate evaluations. COSO explain that the ongoing monitoring activities happen during everyday operations, whereas the amount of separate evaluations is affected by the level of risks and quality of the everyday monitoring activities.

COSO (1994) remind that changing conditions within or outside a company can affect the effectiveness of internal control procedures. They mention that the quality and effectiveness of the internal control procedures must be secured through monitoring. As mentioned above, the ongoing monitoring activities are integrated into the operating activities. The COSO framework remarks that these monitoring activities identify

problems faster than separate controls. COSO argue that, therefore, they should be prioritised. According to COSO, an example of an ongoing monitoring activity is distribution of work where employees check each other's work.

COSO (1994) note, however, that even separate evaluations are needed occasionally. They mention that the controls related to higher risks must be monitored more frequently. COSO explain that the monitoring can be done by the people responsible for the controls, or by internal or external auditors. According to COSO, there are some fundamental guidelines for the monitoring process. First, the evaluator must understand the operating of the whole entity. Second, the true functioning of the system must be determined. Third, he must evaluate the design and results of the evaluation and determine whether the controls are sufficiently effective. According to COSO, documentation of the evaluation can clarify the system's functioning to employees and offer support when presenting the system to external parties. COSO describe that relevant shortcomings in the internal control system should be reported to the person responsible for the control, and to his superior. The framework states, nevertheless, that it can be challenging to define which deficiencies require action. According to Pickett (2012), the onus of the monitoring element lies with the management. He argues that the management must answer the following question: "To what extent can we tell our stakeholders that we have fraud under control and are on a constant watch for any new scams?" (Pickett, 2012, pp. 185).

According to Ahokas (2012), the COSO framework's essential message is that the different components of internal control are interrelated and that the process should be integrated into the whole organisation. Furthermore, she remarks that all five parts are necessary for every company's internal control process. Ahokas notes that the implementation of the components can, however, vary between organisations. Moreover, Ahokas argues that the COSO framework is a good starting point for building and improving an internal control system.

3.3 Sarbanes-Oxley Act

Wikland (2014) describes that the Sarbanes-Oxley Act (SOX), which took effect in 2002, requires the companies listed on American Stock Exchange to prove the quality of their internal control regarding financial statements. Marshall et al. (2006) specify that internal control assessment is addressed in the Act's section 404. According to Marshall et al., the earlier described COSO framework is an example of a framework that is considered to fulfil the Act's internal control requirements. Heir, Dugan and Sayers (2005) mention that SOX defines the regulation of management's evaluation of internal controls in the annual reports. Moreover, Wikland (2014) notes that SOX clarifies that the onus is on the management to maintain efficient internal control. Furthermore, he mentions that SOX introduced significant potential punishments for insufficient internal control, extending to prison sentence. Wikland amplifies that later, in 2005, the U.S. Securities and Exchange Commission (SEC) specified that the controls should focus on those areas within the company which involve the greatest risks. Heir et al. (2005) argue that the development of SOX was started by large financial scandals, such as the Enron scandal, and the unstable market in the USA. In accordance with Heir et al (2005), Marshall et al. (2006) mention that the cases of claimed corporate accounting and financial fraud led to the development of SOX. Moreover, Marshall et al. describe that the varied requirements of the act were established in order to reset trust in corporate reporting.

Marshall et al. (2006) mention that companies which currently lack a risk management framework can use the SOX in establishing an efficient process. Risk management is discussed more in detail in chapter four. Marshall et al. argue that it is essential that companies seek to integrate the demands of the regulation in the risk management processes in a way that leads to added value for the company, instead of merely filling the legal requirements. Sinnett (2009) criticises, however, the regulation and notes that it has failed to eliminate fraud. He demonstrates the claim by examples of new failures and scandals and a comment made by Dennis R. Beresford, a former chairman of Financial Accounting Standards Board, in an interview where Beresford wondered whether the SOX had even decreased fraud.

3.4 Limitations of Internal Control

COSO (1994) remind that internal control has its limitations. According to the COSO framework, "Internal control, no matter how well designed or operated, can provide only reasonable assurance to management and board of directors regarding achievement of an entity's objectives." (COSO, 1994, pp. 79). That is, internal control aims to secure that a company operates on a satisfying level but cannot offer absolute assurance that no risk will occur. COSO (1994) describe that internal control is based on decisions which rely on human judgement. COSO argues that, therefore, there are limitations. COSO mention that one problem caused by human judgement is breakdowns; that is, personnel can misinterpret instructions or for example fatigue can cause errors. According to COSO, another issue is so called "management override"; that is, that management deviates from the company policies or procedures for fraudulent reasons. In addition, COSO note that internal control can miss collusion between internal or internal and external parties. Moreover, Dimitrijevic et al. (2015) describe that collusion enables avoiding the controls and impair the internal control procedures. Finally, COSO (1994) mention that balancing the benefits and costs can be challenging. COSO note however, that companies should aim to find the ideal balance between the costs and benefits. Zakaria et al., (2016) highlight the same above-mentioned difficulties related the internal control.

Moreover, Maijoor (2000) criticises broad internal control definitions, such as the COSO framework, because it is difficult to specify what is internal control and what is not. Spira and Page (2003) also remark the difficulty in outlining internal control. Maijoor (2000) argues that this could lead to all actions within an organisation to be identified as part of the internal control process. Maijoor concludes that the variation in definitions has led to a disconnected internal control research field. Moreover, Spira and Page (2003) refer to Maijoor's (2000) findings and conclude that insufficient research of internal control has led to decisions based on assumptions which lack scientific proof. In addition, Heir et al. (2005) mention the issue of unclear division of responsibility and lack of practical guidance concerning implementation in the COSO framework. Pickett (2012) notes that some claim the COSO framework to be outmoded. He argues, nevertheless, that the framework is still useful to most, especially large, companies.

4 Risk Management

In this chapter, the concept of risk management is discussed. In the beginning of the chapter a definition and development of risk management are presented. Thereafter, the concept of risk appetite is described. After this, the implementation process is described. Then, the risk management process in described in more detail. Finally, in the end of the chapter, challenges related to risk management are discussed.

Merna and Al-Thani (2008) describe that the concept of risk consists of four elements. The first element is the likelihood of incidence. The second element is the level of impact. The third element is tendency to volatility and external influence. The fourth element is the linkage with other risk factors. Merna and Al-Thani claim that a risk always includes all the above mentioned four elements. Moreover, they underline that the correct definition of risk is a crucial part of the risk management process. Merna and Al-Thani (2008) describe that, according to Smith et al. (2006), some risks are known and the likelihood that the risk occurs can be calculated. They note, nevertheless, that other risks are unknown, that is, it is not possibly to calculate the probability of the risk. Merna and Al-Thani (2008) specify that there are several different categories of risks. The fraud risk that is discussed in this thesis is only one of many risks that companies encounter.

According to Spira and Page (2003), risk management has its roots in the pre-modern era where risk was associated with natural events. The definition has, however, largely expanded later. Merna and Al-Thahi (2008, pp. 2) define risk management as “a formal process that enables the identification, assessment, planning and management of risks”. They argue that the goal of risk management is to define company specific risks and prepare for them in a suitable manner. Spira and Page (2003) claim that an assumption in risk management is that company’s risks are identifiable, quantifiable and manageable. In accordance with this claim, Merna and Al-Thani (2008) list the following three aims of risk management: identification of the risks, objective analysis of the risks and response to them. Lam (2006) mentions that risk management helps to prepare for the downside risks, but also to control the financial uncertainties and future business. He explains that companies must identify different possible future scenarios and define the

accepted risk level, also called risk appetite. The concept of risk appetite is explained in more detail later in this chapter. Furthermore, he notes that companies should develop a survival strategy in case a risk occurs.

Lam (2006) describes that the importance of risk management has increased in the last years. Furthermore, he explains that nowadays risk management has become recognised in several fields as an important activity, whereas earlier it was mostly related to banking. In addition, Lam emphasises that risk management has become a company-wide function, while earlier the different types of risks were often managed by varied functions. Lam describes that, for instance, corporate scandals, regulatory requirements and positive examples of other companies are factors that have made risk management widely spread in the corporate world. In addition, he describes that to promote risk management, industries have published guidelines of best practices. The Treadway commission, for instance, established the COSO framework due to concerns related to fraud and corporate governance (Arwinge et al., 2013).

4.1 Risk Appetite

Merna and Al-Thani (2008) claim that there is no one way to categorise people or companies according to behaviour related to risk. They mention, however, that broad grouping is often made. This broad grouping if often referred to as ‘risk appetite’. Risk appetite refers to a company’s tolerance of risks (Lam, 2006). According to Lam (2006), a company’s risk appetite indicates the company’s limits related to risk taking. Moreover, Arwinge et al. (2013) argue that it is necessary that management clearly defines their risk appetite. Merna and Al-Thani (2008) describe that in utility theory risk attitudes are divided into three profiles: risk seeking, risk averse and risk neutral profile. They describe that a risk seeking company is willing to take high risks in order to obtain a possible high win, while a risk averse company prefers low risk. According to Merna and Al-Thani, risk neutral company is a profile in between the two other profiles and is indifferent of the risk. Merna and Al-Thani argue that with the profiles the utility theory describes how people deviate from the most rational decision. Pickett (2012) reminds, however, that the

risk appetite is a subjective concept and can therefore have varied meanings for individuals.

4.2 Implementation of risk management

Lam (2006) explains that to achieve an effective risk management which acknowledges varied risks companies must have an implementation plan. He argues that a risk management framework and implementation plan enable companies to create a consistent and integrated approach concerning risk management. Lam underlines that the framework must cover corporate governance, line management, portfolio management, risk transfer, risk analytics, data and technology resources, and stakeholder management. He argues that these are the key elements of risk management and internal control. Marshall et al. (2006) mention that in 2004 COSO introduced a risk management framework called the COSO ERM framework. They describe that the five elements found in most risk frameworks are: risk definition, risk measurement, risk monitoring, risk allocation and risk management. Similar to the COSO framework for internal control described in chapter 3, the different elements are interlinked and affect each other. Marshall et al. argue that the quality of the process increases over time as understanding of the faced risks increases.

According to Lam (2006), the four stages of risk management implementation are establishing the foundation, identifying and assessing the risks, measuring and reporting the risks, and finally mitigating and managing the risks. As mentioned in chapter three, assessment of risks is a component in the COSO framework. Lam (2006) underlines that the different stages can be performed in various orders. Moreover, he argues that companies should identify the order that fits them best. According to Merna and Al-Thani (2008), the following three questions create basis for the risk assessment process: can something ‘bad’ happen, how likely is it and what are the consequences if it happens. They comment, however, that risk assessors must clarify what the ‘bad’ is for each company.

4.3 Risk management process

Merna and Al-Thani (2008) summarise the risk management process into three main steps: risk identification, risk quantification and analysis, and risk response. They describe that the first step, risk identification, includes decisions of the relevant risks and their specialities. Moreover, Pickett (2012) reasons that if a company manages to identify all relevant risks it can also prepare for and aim to prevent them. Merna and Al-Thani (2008) underscore that the risk identification process must be repeated regularly.

According to Merna and Al-Thani (2008) the second step, risk quantification and analysis, consists of estimation of the risks that were identified in the previous step. Merna and Al-Thani describe that the goal of the risk analysis is to determine the relevant risks which the company must address. They note that risk analysis can be made using both qualitative and quantitative techniques. Merna and Al-Thani specify that qualitative methods aim to estimate the effects that the different risks create. They explain that the importance of the risk is evaluated based on the possible effects. According to Merna and Al-Thani, for instance brainstorming, assumption analysis, risk registers and interviews are examples of qualitative techniques. Merna and Al-Thani describe that the quantitative methods in turn, focus on calculating exact values and probabilities on the projects. Merna and Al-Thani mention that quantitative techniques usually require statistical data, which is then analysed with the help of computer models. According to Merna and Al-Thani, for instance decisions trees, Probability-Impact grid analysis and sensitivity analysis are examples of quantitative techniques.

Merna and Al-Thani (2008) describe that the third and final step, risk response, includes the concrete reactions to the identified and analysed risks. Merna and Al-Thani argue that there are four possible actions in this part. Companies can, for example, eliminate a risk or decrease it. Third option is to transfer some risks to different stakeholders. Finally, the fourth possibility that Merna and Al-Thani highlight is to not react to the risk and retain the risk. They note that unresponsiveness can be caused by, for instance, a failure in the preceding steps. Pickett (2012) adds to the above-mentioned steps and mentions that in fraud risk management companies must also have ongoing detection routines. He argues

that controls alone are insufficient. Pickett underlines that, for instance in the case of fraud, companies must actively search for possible frauds.

4.4. Challenges in risk management

Lam (2006) underlines that there are various issues and difficulties related to implementation and usage of risk management. According to Lam, many companies tend to produce low quality risk reports. He explains that the reports often include a large amount of irrelevant data. He accentuates that it is crucial that risk management provides clear and relevant information to the management. Lam notes that another challenge in risk management is insufficient communication and coordination. Lam mentions that the roles of different functions must be clearly assigned to avoid blind spots. Moreover, he describes that the implementation process can be deficient in the right resources. Lam emphasises that the implementation process requires a large amount of resources and can cause great costs for the company. Furthermore, according to Lam, it is essential to provide evidence of early benefits in order to justify and motivate the support from the management and other stakeholders. Regardless the challenges, Lam (2006) argues that risk management will be widely used also in the future.

5 Previous research

In this chapter, previous studies of internal control and fraud are presented. First, studies which focus on internal control's effect on the risk of fraud are presented. Thereafter, studies which focus on internal control's role in fraud detection are presented.

5.1 Internal control's effect on the risk of fraud

Rae and Subramaniam (2008) study in their article "Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud" the connection between theoretical concepts of organisational justice, internal control and fraud literature. They aim to develop models for employee fraud and quality of internal controls. They describe that the data for the study were collected with a survey which was sent to Australian companies in different fields. They received a total of 64 replies. The study's first model, which tests employee fraud, hypothesises, in line with the fraud triangle, that employee fraud arises when both motivation and opportunity occur due to ineffective internal controls. Rae and Subramaniam examined the model with a logistic regression analysis. The study's second model, which tests the quality of internal controls, hypothesises that corporate ethical environment, risk management training and internal audit activities affect the quality of internal control. Rae and Subramaniam examined this model examined with a multiple regression analysis. Rae and Subramaniam's findings related to the first model suggest that effective internal control limits the relationship between perceived organisational justice and employee fraud. Thus, the findings support the fraud triangle theory. Furthermore, the findings related to the second model signal a positive connection between internal control quality and three elements: corporate ethical environment, risk management training of staff and level of internal audit.

Shanmugam, Haat and Ali (2012) research internal control and fraud prevention in Small and Medium sized enterprises (SMEs) in Malaysia. They examined literature and previous studies within the field. Shanmugam et al. mention that SMEs tend to be more

vulnerable to fraud and that it is more difficult for them to overcome the loss. Shanmugam et al. mention that previous studies indicate a relationship between effective internal control and decreased fraud within companies. Moreover, they describe that, in the studies they examined, fraud occurred when opportunity or financial pressure existed. They also noticed that, in some studies, the internal audit function was missing in the companies where fraud was committed. Even Petersen, Bruwer and Le Roux (2018) studied internal fraud and internal control in SMEs. Equivalent to Shanmugam et al.'s (2012) study, Petersen et al. (2018) conducted a non-empirical study which reviewed literature and previous studies. They reviewed a total of 100 sources. In line with Shanmugam et al. (2012), also Petersen et al. (2018) found a theoretical relationship between internal control and fraud risk. Their analyses indicate, however, that SMEs tend to use ineffective internal control procedures which fail to alleviate the probability of fraud.

Donelson, Ege and McInnis (2017) study in their article "Internal Control Weaknesses and Financial Reporting Fraud" the relationship between weak internal controls and the risk of financial reporting fraud committed by the top management. The study was conducted by examining the relationship between material weaknesses and fraud revealed in the following years. Donelson et al. describe that material weaknesses refer to an audit opinion under the SOX regulation; in case of a material weakness the auditor has remarked weakness in one or several internal control procedures. Donelson et al. collected the initial sample of auditor internal control opinions from Audit Analytics database. The fraud cases were gathered from the Federal Securities Regulations Database and RiskMetrics. Donelson et al. describe that the fraud cases consist of settled securities class-action lawsuits which allege violations of GAAP, and enforcement actions by SEC and Department of Justice which allege fraud or other intentional accounting misconduct. Donelson et al. gathered a total of 127 cases. They analysed the data with a logistic regression and a propensity score matched-pairs test. The results of the tests indicate that there is a strong link between material weaknesses and future financial statement fraud revelation. Donelson et al. specify that, according to the results, the material weaknesses which occur on an entity level, rather than process level, are strong signals of possible future financial statement fraud revelation. Finally, Donelson et al. argue that the results of their study signal that SOX offers a system which perhaps facilitates early detection of possible future fraud cases.

Puspasari and Suwardi (2016) investigate in their article "The effect of individual morality and internal control on the propensity to commit fraud: evidence from local governments" how employees' morality and existence of internal controls link to likelihood of fraud in public sector. Puspasari and Suwardi performed the study as experimental research. The study was conducted in Indonesia where, according to Puspasari and Suwardi, the level of corruption is high. They asked 57 master's students to complete two assignments to assess the linkage between morality, internal control and fraud risk. The first test examined level of morality while the second test focused on assessing the participant's likelihood to commit internal fraud. Puspasari and Suwardi's study indicates that both the participants' morality and existence of internal control affect the risk of fraud. According to Puspasari and Suwardi's results, the participants with low level of morality were less likely to commit fraud if there was an internal control in place. The likelihood of committing fraud by a participant with high level of morality, however, was unaffected in case of missing internal controls. Puspasari and Suwardi's study signals that internal control can decrease the risk of fraud.

Nawawi and Salin (2018) identify in their article "Internal control and employees' occupational fraud on expenditure claims" weaknesses in the internal control procedures. Moreover, their study examines employees' attitudes related to internal fraud. They also assess if the working environment reduces risk of internal fraud. The study was conducted as a case study and it studied one Malaysian company with an outsourced internal control department. According to Nawawi and Salin, the data were collected through document analysis and a questionnaire sent to 35 employees. Nawawi and Salin found that the procedure of expenditure claims had weak internal controls and was exploited in the company. Moreover, they describe that the questionnaire results showed that falsifying costs, such as reporting false kilometres for cost compensation, were the most common fraud within the company. Similar to Pusapari and Suwardi's (2016) study, Nawawi and Salin (2018) found signals that stronger internal controls could reduce the fraud risk. What is more, Nawawi and Salin's study indicates that company culture and environment within the company, as well as level of dissatisfaction, affect the likelihood of fraud.

Barra (2010) approaches the linkage of internal control and fraud from a different perspective. Barra's article "The Impact of Internal Controls and Penalties on Fraud" studies the role of internal control but also the role of penalties in the fraud prevention process. Barra has an analytical approach and she creates two analytical models, one with employee perspective and another with company perspective. Barra argues that, on the one hand, the employee model indicates that when committing fraud requires more effort employees will want to steal more to make it profitable to commit fraud. According to Barra, the firm model, on the other hand, is based on the assumption that companies want to minimise the cost of fraud. Barra notes that, as also described in the COSO framework in chapter 3, it can be "cheaper" to let smaller fraud happen. According to Barra's two analytical models, due to penalties and internal controls fraudsters must be able to steal a larger amount of money to keep the fraud as an attractive option. Barra's models recommend using internal controls as preventive measures for non-managerial employees, whereas penalties are recommended for managerial employees. More specifically, Barra's study indicates that internal controls are more efficient in increasing the effort to commit fraud for non-managerial employees, whereas for managerial employees it is easier to bypass the controls. According to the analytical models, penalties are a more efficient option to prevent managerial fraud. Thus, the article supports the American SOX regulation that imposes high penalties on managers.

Zakaria, Nawawi and Salin (2016) study in their article "Internal controls and fraud – empirical evidence from oil and gas company" internal control weaknesses in an oil and gas company in Malaysia and the weaknesses' possible connection to fraud risk in the company. They focused in one company and conducted a case study. They collected the data through interviews with senior management and internal auditors, as well as through documents from internal audit procedures. Their study indicates that the identified weaknesses affect the likelihood of fraud within the company. Zakaria et al. underline that weaknesses in oversight and documentation increased the fraud risk the most. The interviews with internal auditors highlighted weaknesses in daily control procedures. The study indicates that weak or missing internal controls create an opportunity to commit fraud. Therefore, as the fraud triangle's opportunity element increases also the risk of fraud increases. Although the study focusses only on one company, its results are in line

with the results from other previous studies described above. Thus, the results can be considered relevant even for other companies.

Mirinaviciene (2014) analyses in her article "Internal control and fraud prevention: prior research analysis" the findings of 11 previous studies in the field of internal control and fraud. The studies use varied sources of data and analysis techniques. In line with the findings of the above described other previous studies, also Mirinaviciene found that the majority of the studies she analysed indicate that internal control improves the prevention and detection of fraud. Moreover, she argues that the studies indicate that companies can use internal control to reduce the likelihood of fraud and costs related to fraud. Mirinaviciene emphasises that simultaneous use of varied fraud prevention measures is considered the most effective tool against fraud. She underscores that external audits are less effective in preventing and detecting fraud. Mirinaviciene argues that although most companies focus on detecting fraud, it is more profitable to focus on preventing fraud.

All studies described above found a connection between internal control and likelihood of fraud. Some studies (Petersen et al., 2018; Puspasari and Suwardi, 2016; Mirinaviciene, 2014; Shanmugam et al., 2012; Barra, 2010; Rae and Subramaniam, 2008) indicate that existing internal controls decreased the risk of fraud, whereas other studies (Nawawi and Salin, 2018; Donelson et al., 2017; Zakaria et al. 2016) signal that weak or non-existing internal control procedures increased the likelihood of fraud in the company. According to the ACFE (2018a) Report to the Nations, the size of the company affects the likelihood of missing internal controls causing fraud. ACFE's report describes that in smaller companies with less than 100 employees missing internal controls were the cause of fraud in 42% of the cases. Companies with over 100 employees appear to be better protected by internal controls as poor internal controls caused only 25% of the frauds. While internal control was found to have an effect on the risk of fraud in all studies, also other factors, such as amount of penalties (Barra, 2010), company culture and perceived organisational justice (Nawawi and Salin, 2018; Rae and Subramaniam, 2008) and level of morality (Puspasari and Suwardi, 2016), were found to affect the likelihood of fraud.

5.2 Detection of fraud

Based on the earlier described studies, preventive measures are considered essential in curbing fraud. Some studies focus, nonetheless, on the detection of fraud. Even the detective measures can be considered relevant since they increase the risk of "getting caught" which is linked to, for instance, the opportunity factor of fraud triangle. In line with Shanmugam et al.'s (2012) remark of the missing internal audit in cases of fraud, Westhausen (2017) emphasises the importance of internal audit function in his article "The escalating relevance of internal auditing as anti-fraud control". Westhausen examines international standards of professional practice of internal audit and internal audit practices within companies. The empirical data on internal audit practices was obtained from fraud reports and previous studies. He underscores that in ACFE's Report to the Nations 2016 internal audit was the second most common fraud detection source. Even the Report to the Nations 2018 lists internal audit as the second most common fraud detection source (ACFE, 2018a). Furthermore, Westhausen (2017) describes that fraud's importance as a strategic topic has increased. According to the article, for instance, internal audit institutions have published standards and offered conferences and training related to fraud. Nonetheless, the article highlights some areas of improvement for internal audit, such as identifying weak or missing controls, overconfidence and taking too much or not enough responsibility.

In addition to the internal audit function, also employee training is argued to increase the number of frauds detected. Abiola and Oyewole (2013) study in their article "Internal Control System on Fraud Detection: Nigeria Experience" how internal control procedures affect the likelihood of fraud detection in banks. They analysed data collected from 10 banks in Nigeria. The data were gathered with questionnaires sent to employees in managerial positions as well as through varied accounts and reports. Abiola and Oyewole's study indicates that internal control has a significant effect on fraud detection in banks. Moreover, the results signal that employee training in general, as well as training specifically on internal controls, increased the fraud detection effectiveness.

Westhausen (2017) and Abiola and Oyewole (2013) highlight internal audit function and internal control in general, as well as employee training, as effective detective measures. PwC's (2018) "Global Economic Crime and Fraud Survey 2018" also indicates that internal control has a significant role in fraud detection. According to the PwC survey, 52 per cent of the most disruptive fraud or economic crimes were initially detected through internal control. PwC (2018, pp.26) note that internal audit routine was the most effective control, followed by fraud risk management and monitoring suspicious activity. PwC also mention corporate security, data analytics and rotation of personnel as controls that detected fraud, although a smaller percentage of frauds were detected with these controls.

According to ACFE's (2018a) Report to the Nations, whistleblowing is, nevertheless, the most common way of detecting fraud. Transparency International (2019a) define whistleblowing as "making a disclosure in the public interest by an employee, director or external person, in an attempt to reveal neglect or abuses within the activities of an organisation, government body or company (or one of its business partners) that threaten public interest, its integrity and reputation." ACFE (2018a) describe that up to 40 per cent of internal frauds were detected due to a tip from a whistle-blower. Moreover, ACFE remark that in 53 per cent of the cases the reporter was an employee. ACFE note that of the internal fraud types corruption was most likely detected by a tip from a whistle-blower as up to 50 per cent of corruption cases were detected with the help of a whistle-blower. According to ACFE, asset misappropriation and financial statement fraud were detected by a tip from a whistle-blower in 38 per cent of the cases. A whistle-blowers' position is often problematic. According to Transparency International (2013), in 2013 majority of the European countries were lacking a sufficient legal framework to protect whistle-blowers. Transparency International note that many whistle-blowers risk, for instance, losing their job after the disclosure. Transparency International argue that it is essential that better legal frameworks will be implemented to encourage and support whistleblowing. Most studies stress the importance of preventive measures for the decreasing likelihood of fraud. It may also be valuable for companies to improve the detective measures and increase the number of frauds detected by other means than whistleblowing. This would also affect the opportunity factor of fraud triangle.

6 Method

In this chapter, the empirical section of the thesis is described. First, the background for the empirical study, based on the earlier presented theory and previous research, is discussed. Thereafter, the method of the study is introduced. Then the sample of the study is discussed. Finally, the method for analysis of the data is described.

6.1 Background for the study

According to ACFE's (2018a) Report to the Nations, for example Portugal and Iceland have a lower level of fraud incidents than many other Western European countries. The United Kingdom (UK) has a higher number of fraud incidents. In total 130 fraud cases were reported in Western Europe in 2018 (ACFE 2018a, pp. 73). ACFE illustrate that out of the 130 fraud cases one occurred in Portugal and 34 in the UK, while on average there were approximately eight fraud cases per country. ACFE's report includes 16 Western European countries. ACFE's Report to the Nations demonstrates that there are differences between the European countries in the number of reported fraud cases.

The previous studies described in chapter five indicate that internal control is an effective way to prevent fraud in companies. However, companies tend to use weak or ineffective internal controls in fraud prevention (Petersen et al., 2018; Nawawi and Salin, 2018; Donelson et al, 2017; Zakaria et al., 2016). PwC's (2018) Global Economic Crime and Fraud Survey indicates that in 59 per cent of internal fraud cases the opportunity factor of the fraud triangle theory was the main reason for committing fraud. These findings support the assumption that the risk of fraud could be decreased by targeting the opportunity factor with internal control procedures.

Based on the previous research, the data from ACFE's (2018a) Report to the Nations and PwC's (2018) Global Economic Crime and Fraud Survey, it could be hypothesised that companies which use strong and effective internal controls have a lower risk of fraud.

The following research questions were formulated based on the earlier described theories and previous research:

1. *How do companies use internal control to prevent internal fraud?*
2. *Which types of controls are considered the most effective for internal fraud prevention?*
3. *What are the areas for improvement in preventing internal fraud through internal control?*

Thus, the aim of this study is to observe which types of internal controls companies use and which controls are considered to be the most effective ones in internal fraud prevention in a European context. The study also aims to understand why certain controls are considered the most effective ones for fraud prevention.

6.2 Research method

Research methods can be divided into two main groups: quantitative and qualitative methods. Quantitative methods are often broadly defined as methods which use numerical values in the analysis. Cassell, Buehring, Symon and Johnson (2006) describe that the definition of qualitative methods is often simplified as the opposite of quantitative methods, that is methods that use non-numerical data in the analysis. Cassell et al. (2006) argue that the definition of qualitative methods is more complex than the definition given above. They note that qualitative research is used broadly in various fields and that several different methods are classified under qualitative research. They conclude, nevertheless, that the first mentioned definition, that is, methods of gathering and analysing non-numerical data, is the most common definition in the management field. This thesis uses qualitative research methods. The definition of qualitative research methods given by Cassell et al. (2006) is used in this thesis.

According to Saldaña (2011), one or several methods can be used to collect data in qualitative studies. He mentions that, for instance, interviews, observation, written

surveys and examining documents are examples of data collection methods. In this thesis interviews are used to collect data.

6.3 Interviews

As mentioned above, in this thesis the data is collected through interviews. According to Saldaña (2011), interviews are a popular data collection method in qualitative research as they enable gathering information directly from people. Moreover, he explains that interviews offer information about the interviewees' personal perspectives and experiences. Saldaña notes that in an interview the researcher can encounter new areas to discover and study further.

There are several variations of interview methods. Saldaña (2011) describes that the interview formats vary from spontaneous unstructured interviews to planned and structured interviews. He specifies that in unstructured interviews the researcher may have solely prepared ideas of possible topics to cover whereas in a structured interview the questions and their order are decided in advance. He mentions that, in addition to the structure of the interview, the number of interviewees and interview times can vary.

In addition to the interview format, the researcher must also select the interviewees. Saldaña (2011) explains that the researcher should select interviewees who are relevant for the study and who can provide relevant content to the questions. According to Saldaña, there are varied views on how many interviewees should be included in a study. Some argue that interviewing just one person offers a deeper view of the topic whereas others believe that new interview participants should be included until the new interviewees do not offer any new information. Saldaña underlines that due to for instance time constraints it is impossible to interview every person who is relevant for the topic. Therefore, Saldaña argues that through sampling the interview process becomes feasible.

Saldaña (2011) notes that it is important to prepare well for the interviews. He stresses that the time and location of the interview should be scheduled according to the interviewee's preferences. He explains that it is important that the interviewee is comfortable in the location and that privacy is secured. In addition, Saldaña advices to record the interviews as video or voice recordings. He notes that as some interviewees are uncomfortable with video recording, voice recordings are often more suitable. Moreover, he reminds to secure beforehand that the recording device functions correctly and to also take written notes during the interview. After the interview, the recording should be transcribed. Saldaña argues that the transcription should be written shortly after the interview when it is still fresh in the mind.

The preparation process of the questions for the interview depends on the chosen interview format described earlier in this chapter. Saldaña explains that the more structured interview format is chosen the more preparation of the questions is required. Saldaña (2011) argues that interviews are more likely to flow better if the questions are well prepared beforehand, especially when it is the first interview time. Moreover, he underlines that due to time constraints all the questions must be relevant and contribute to the study. Saldaña advices to avoid questions that suggest a certain answer and questions that can be replied with "yes" or "no". He argues that this limits the input received from interviews. He also notes that the researcher should focus to ask one question at a time and reserve enough time for the participant to reply. Saldaña recommends testing the interview questions on someone else before the interview to confirm the quality of the questions.

For the purposes of this thesis a semi-structured interview style was chosen. The date, the questions and the duration of the interviews were defined beforehand. Both external and internal stakeholders were interviewed to obtain a broader understanding of the topic. The sample of the study is described more in detail in the next section. The interviews were confirmed in varying ways with the participants. The interviewees in group 1 were asked to participate in the study in person and an accompanying letter, presented in appendix 1, was sent later to confirm the dates of the interviews. With one of the interviewees in group 1, the date was agreed in person and no accompanying letter was sent. The interviewees

in group 2 were asked to participate in the study with the accompanying letters presented in appendices 1 and 2. As the interview sample consists of two groups, two sets of interview questions were prepared. Same interview questions were sent to all the interview participants in group 2 to enable better comparison between the different interviews. The questions for group 1 were slightly altered for the participants due to different backgrounds. The interview questions for both groups 1 and 2 were tested beforehand in a test interview with a person who does not participate in the study. The interview questions address questions of the most common and most effective internal controls. The detailed interview questions are disclosed in appendices 3 and 4. The interviews were conducted in English and Finnish depending on the interviewees' preferred language. The interview languages are disclosed in appendix 5. In total, seven people were interviewed. One interview was done in person while four interviews were done via Skype for Business due to logistical reasons. All these interviews were recorded as voice recordings, and the recordings were transcribed shortly after the interviews. The interviews lasted on average 40 minutes. Two interviews were done via email due to interviewees' tight schedules and differences in time zones which did not allow a live interview.

6.4 Sample

Saldaña (2011) argues that triangulation increases a study's credibility. The concepts of credibility and trustworthiness are described later in this chapter. According to Saldaña (2011), triangulation refers to studying a topic from three, or more, perspectives. That is, using various data collection methods or interviewing different stakeholders. In this thesis, the triangulation is implemented through interviewing different sources, that is stakeholders in various positions both inside and outside companies. In total, seven people from four European countries were interviewed. The interviewees were divided into two groups based on whether they are an internal or external stakeholder.

Group 1 consists of people outside companies. More specifically, group 1 consists of two Big 4 accounting firm partners and the deputy CEO of Accountancy Europe. Accountancy Europe unites 51 professional organisations from 36 countries that represent 1 million

qualified accountants, auditors and advisors. The deputy CEO of Accountancy Europe is also a certified public accountant (CPA) in Belgium, the UK and the US. These interviewees selected as they have significant experience in assessing internal controls and can provide an outsider's opinion on various types of companies' internal control processes. Group 2 in turn consists of people inside companies, that is, various profiles from different industries. The internal stakeholders were selected to obtain a more detailed understanding of company specific controls. Different profiles were selected to obtain a broader understanding of internal control procedures within companies. A more detailed description of the interviewees and interviews is presented in appendix 5. Several interviewees wished to remain anonymous due to the sensitivity of the topic or their position within their company. First, to obtain a broader perspective on fraud and internal control from outside the companies, interviewees in group 1 were interviewed. Second, for a viewpoint from within companies, interviewees in group 2 were interviewed.

6.5 Analysis of the interviews

The interview data were analysed to increase the understanding of how companies use internal control to prevent fraud within companies. In addition, the analysis aimed to identify which types of controls are considered to be the most effective. Moreover, the analysis aimed to attain an understanding of why some controls are considered more effective than others; areas for improvement were also analysed.

Saldaña (2011) describes that one way to analyse data from qualitative studies is to construct patterns found in the collected data. He mentions that multiple methods can be used to conduct the analysis. Saldaña underlines that the analysis process commences already during the data collection phase. He describes that the transcription process is the next step in the analysis. Saldaña argues that during the transcription process the researcher's brain starts to process the data. According to Saldaña, transcribing the interviews enables the researcher to perceive a broader view and create connections between the data and theory. He explains that various methods can also be used to support structuring the data.

In this thesis, the interview transcriptions were analysed to construct patterns in the interviews. The aim of the pattern construction is to identify similarities in the interviews and identify whether interviewees have similar experiences and observations. Saldaña (2011) describes that category construction is a method which allows the researcher to organise and analyse the data. He argues that categorising the data into larger units simplifies identification of characteristics and possible connections between categories. Saldaña describes that, on a more detailed level, there are various different methods for analysing the data from interviews. In this thesis, the data were analysed with descriptive coding. Saldaña (2011) specifies that the method of descriptive coding aims to summarise the main content of interview's different sections into a few words. The code words are then categorised.

In the analysis process of this thesis, the transcriptions were first analysed and processed on a general level and the most relevant content was highlighted. Then, the interview transcriptions were coded with descriptive coding to better grasp the collected data. After this, the codes were grouped into more general categories to construct patterns in the interviewees' answers. The analysis resulted in a total of 20 categories.

6.6 Credibility and trustworthiness

Saldaña (2011) describes that researchers should consider the concepts of credibility and trustworthiness during the research process and when writing about the results. Saldaña explains that the concept of credibility in qualitative research refers to how convincing the study is. That is, the credibility of the study represents how believable the readers consider the study's results and conclusions. Lincoln and Guba (1985) describe that to achieve credibility, researchers must ensure that they perform the research in a way that improves the likelihood that the results will be considered believable. According to Lincoln and Guba, researchers can enhance credibility through adequate time spent in data collection. Lincoln and Guba refer to this as prolonged engagement. Another measure that Lincoln and Guba describe is persistent observation, that is, focus on the most significant factors which affect the studied issue. Third measure is triangulation which is described earlier in this chapter. Lincoln and Guba argue that researchers can

also improve a qualitative study's credibility by having respondents check the results. Saldaña (2011) also lists factors that affect a study's credibility. He names that, as a basis, the most relevant publications must be included in the theory and previous studies. In addition, he argues that presenting the data analysis method and using a variety of data collection methods increase credibility. Even quoting interviewees strengthens credibility.

The other important concept in qualitative research is trustworthiness. Lincoln and Guba (1985) describe that trustworthiness consists of the concepts of credibility, transferability, dependability and confirmability. Saldaña (2011) describes that there are various ways to increase trustworthiness. He mentions that, for example, disclosing the lengths of field work and interviews or specifying the amount of gathered data are measures to improve trustworthiness. Saldaña emphasises that the key to achieve credibility and trustworthiness is transparency and honesty during the research and writing process.

7 Results

In this chapter, the results of the interviews are presented. The results are divided into three sections, based on the research questions presented in chapter 6 and the interview guides presented in appendices 3 and 4. First, the responses related to questions on fraud are presented. Thereafter, the responses on questions on use of internal control are addressed. Finally, the responses on questions related to effectiveness and improving of internal control in fraud prevention are presented. In each section the results from group 1, that is respondents outside companies, and group 2, that is respondents inside companies, are presented separately.

7.1 Significance of fraud

7.1.1 Group 1

All three interviewees in group 1 thought that fraud is a significant issue and can cause various types of damage to companies. Blomme mentioned that, in addition to the direct costs, fraud can result in indirect costs for companies. She explained that fraud can interfere with a company's operations and lead to reputational damage. Both Thompson and Partner A underlined that minor fraud is very common in companies, whereas significant fraud cases that lead to large damage occur less often. Furthermore, Partner A believes that majority of the minor fraud is never detected. He also described that the more significant frauds happen on the top management level.

The interviewees also noted that various factors affect the fraud risk and the potential damage in companies. All the interviewees mentioned that industry affects the type of fraud. Both Blomme and Thompson described that the fraud risk increases when incentive and opportunity to gain benefit exist. In addition, Partner A argued that the risk of fraud reflects the values of society. Thompson also mentioned that geographical location affects the risk. Thompson noted that even performance pressure can increase the risk of fraud.

7.1.2 Group 2

Interviewee A said that fraud is a significant risk for her company. Interviewees B, C and D believed that their companies have a low risk of fraud. Both interviewees A and C described that the large size of their companies increase the risk of fraud. Both mentioned that the large number of employees increases the risk of fraud. Interviewee B noted that the risk of fraud is low due to strict regulation and controls related to fraud in the financial industry. Interviewee D described that her company is large enough to have solid processes and internal control. At the same time, the company is small enough for people to know one another and to be aware of what happens in different parts of the organisation, which lowers the risk of fraud.

Interviewee C described that fraud would cause limited damage to her company due to strong internal controls. She believes that something exceptional would be caught by the controls very quickly. Interviewees A, B and D mentioned that fraud within their companies could cause direct as well as various types of indirect damage. Interviewee A specified that fraud could, for example, affect the company's stock exchange rate. According to interviewee B, fraud could affect the company's reputation and clients might lose their trust in the company. Interviewee D, in turn, mentioned that internal fraud could cause damage to relations with banks and suppliers. In addition, she described that hiring new personnel to replace the fraudster would create costs.

Interviewees A and C mentioned that their companies had had cases of internal fraud. In interviewee A's company the fraudsters had bought goods for their own use and charged the employer, whereas in interviewee C's company, two employees had colluded and fabricated false invoices. In both companies the fraud cases were reported to the police and the related control procedures were revaluated.

7.2 Use of internal control

7.2.1 Group 1

All the interviewees emphasised that there are large differences in internal control between companies. The interviewees mentioned that company specific level of risk affects how much companies invest in internal control. According to the interviewees, especially size and industry affect the level and use of internal control. Blomme underlined that also smaller companies have internal control, but that it is often more limited than in larger companies. Both Blomme and Thompson explained that smaller companies often use basic controls based on common sense, rather than any framework. All interviewees in group 1 mentioned that segregation of duties is a basic control that even the smallest companies aim to have. In addition to segregation of duties, Blomme and Thompson listed that authorisations and access rights controls are basic controls that are used even in small companies. Both Blomme and Thompson pointed out that due to digitalisation, even smaller companies tend to have built-in controls in their IT systems. Blomme remarked that this has made more controls common also in small companies.

The above-mentioned diversity in level and use on internal control was also illustrated in the responses on the use of the COSO framework. According to the interviewees, the COSO framework for internal control is, on the one hand, rarely used in small companies due to its complexity. All the interviewees in group 1 described that in large companies, on the other hand, the COSO framework is widely used. Thompson specified that some companies use it fully, but many tend to pick the pieces that are most relevant for their business. Blomme noted that companies adapt the COSO framework to their environment and thus it looks different between companies. She also mentioned that some systems might be based on the COSO framework, although they are not referred to as the COSO framework. In addition, the level of risk affects the use of the internal audit function. More specifically, the interviewees mentioned that internal audit is a function that is mostly seen in large companies. Partner A noted, however, that some smaller companies that operate under regulatory requirements also have the internal audit function in use.

All the interviewees in group 1 noted that the control environment sets a ground for the whole internal control process. Blomme noted that sometimes this is communicated by a code of conduct but more often it is referred to as the 'tone at the top'. Furthermore, Thompson specified that the tone at the top determines the tone for implementation of the controls throughout the company.

In relation to the number of controls, the interviewees emphasised that it is impossible to determine, as controls can go up to thousands in large companies. Blomme mentioned that the larger the company is, the more they rely on controls and try to automate processes. In addition to the previously mentioned controls, the interviewees mentioned that preventive controls in general are common in companies. Regarding detective controls, measurement review controls, KPIs and management review controls were mentioned as common controls.

7.2.2 Group 2

The results from the interviews in group 2 indicate that there are large differences in internal control between the four companies. Regarding the use of the COSO framework, only interviewee C said that her company uses the COSO framework for internal control. She specified that the COSO framework is fully implemented in her company. Interviewees B and D mentioned that their companies do not use the COSO framework. According to B, his company's internal control is based on regulatory framework for insurance. Interviewee D in turn explained that her company's internal control is based on their own analysis of risks and necessary control functions. Interviewee A was not aware whether her company uses the COSO framework or another internal control framework.

More specifically on the design on internal control, interviewees B and C explained that they use three lines of defence for their internal control. In both companies, the first line is formed of different operative departments that handle the operative risk. The second line of defence is a companywide, independent risk management function. Finally, the third line of defence is an internal audit function. Interviewee A also mentioned that her

company has an internal audit function. Interviewee D noted that internal audit function would be an improvement to their internal control.

Regarding the number of controls, all the interviewees in group 2 said that it is difficult to calculate how many controls they have in total. Interviewee C noted that they have thousands of controls throughout the company. In addition, interviewee B explained that they have numerous controls, but they are divided into the following three categories: identifying and assessing risks, measuring risks, and monitoring and reporting the risks. Some control activities were mentioned in several interviews in group 2. Interviewees A, C and D said that their companies use access rights controls, authorisations, approval rights and code of conduct. In addition, interviewee C underlined that the four-eyes-principle, which prevents one employee from acting alone, is used in their processes. Interviewees A and D also mentioned that they use the four-eyes-principle in, for example, payment processes. Moreover, interviewees A and D mentioned that they use segregation of duties. Interviewee C remarked that although they aim for segregation of duties, it is challenging because they only have a few employees in her department. In addition to the above-mentioned controls, interviewee A said that they have rotation of personnel in place and interviewees B and C mentioned that their companies use management overview controls. Interviewee C added that they use KPIs.

The responses in group 2 indicate that internal control has an important role in the companies' procedures. Interviewees A and C specified that they mainly use preventive controls and that they have strict rules on who can do what within the company. Interviewee C described that risks are assessed and measured on a continuous basis. In addition, interviewee A explained that the importance of internal control is a common thread throughout the processes and that the controls are mainly built in the systems and processes. Interviewee D also mentioned that their processes are built to entail segregation of duties and controls for approval rights. Both interviewees A and C described that they have regular e-learnings and tests on their companies' policies and code of conduct.

7.3 Effectiveness and improving of internal control in fraud prevention

7.3.1 Group 1

The responses in group 1 indicate that effective internal control consists of various elements. All interviewees in group 1 stressed that the key to effective internal control is right company culture. Blomme described that "*if company management give the impression in some way that internal control is not important, or that they actually bypass controls – that is the worst you can have. Even though you have the best system, it will not help you.*" Furthermore, Thompson emphasised that if the tone at the top implies that control procedures can be ignored, they will be. Also Partner A underlined that the top management must communicate the importance of the controls. Moreover, he described that the culture must be right throughout the company, that is, everyone must aim for a functioning internal control. All the interviewees concluded that the message from the top must be that fraud is taken seriously. In addition, Blomme added that a clear company structure and assignment of responsibilities are important.

Regarding the controls, the interviewees thought that, in general, preventive controls are most effective in the fight against fraud. Thompson explained that they are detailed enough to stop fraud whereas detective controls only work once something has already happened. He specified that built-in controls that stop the process without, for example, right authorisations or access rights are effective. He remarked, however, that the controls should be appropriate in relation to the risk in order to avoid stopping the business. Partner A stressed the importance of rotation of personnel. Both Partner A and Thompson mentioned that experienced people in trusted positions are more likely to commit fraud. Blomme noted that, on the detection side, whistleblowing is the most common way to detect fraud.

In addition to the control environment and control activities, also other significant elements were identified. Blomme emphasised the importance of properly designed internal control. Both Blomme and Thompson mentioned that most companies hire an

external consult to help implement the internal control. Blomme noted that it is important to include internal people in the process to ensure that the internal control addresses company specific risk factors. She added that it is crucial to understand how the controls work and to ensure that they address the right risks. In addition to the implementation, Blomme underlined that the controls must be enforced. Moreover, she specified that companies must ensure that the controls cannot be circumvented. All the interviewees mentioned that the controls should be monitored and revaluated regularly. Blomme described that it is essential to update the controls at the same time as processes are updated. Moreover, Partner A stressed that *"internal control has to be maintained, all the time.*" Partner A suggested that regulatory evaluations of internal control by a third party could improve internal control's effectivity.

Besides the effectiveness of internal control, the interviewees also identified weaknesses related to internal control. Thompson described that overreliance on imprecise controls and on certain individuals is a common weakness in companies' internal controls. In addition, Blomme mentioned that people struggle to believe that there can be fraud in their company. Moreover, Thompson and Partner A noted that people often cannot believe that the most trusted people in the company would commit fraud. Thompson noted that management override of controls and collusion continue to create issues in internal control. In addition to internal fraud, Blomme and Thompson commented that digitalisation has increased the risk of external fraud in the form of cybercrime. All the interviewees remarked that fraud can never be fully eliminated. In addition, they mentioned that the cost and benefit relationship should be considered. The interviewees specified that internal control should not create more costs than fraud would. Thompson argued that companies can best prevent fraud through elimination of incentive and opportunity.

7.3.2 Group 2

Responses in group 2 indicate that different types of preventive controls are considered to be the most effective types of controls. Interviewees A and C mentioned that controls that are built in the IT systems and in the processes are the most effective types of controls.

Both interviewees A and C explained that these types of controls would effectively prevent fraud as people can only have access to what they are supposed to within their role. Interviewee A acknowledged that the controls slow the company's processes. She argued, however, that the benefit of the controls was higher than the nuisance. Moreover, interviewee B mentioned that segregation of duties, which ensures that an individual cannot make a process go forward alone, is effective. In addition, interviewee D argued that systematic, regular and automatic controls, such as processes, approval rights and checks, as well as access and user rights controls, are effective.

Besides the effective controls, the interviewees also identified weak controls. Interviewee A described that guidelines and advice are the weakest types of internal control as they are easy to bypass. In addition, interviewee C mentioned that instructions that people need to remember in order to follow are ineffective. Interviewee D described that trust and ignorance make controls ineffective. She specified that management's non-interest in designing and implementing internal control can result in only one person deciding on internal control, which she argued to be risky. In order for internal control to be effective, on the other hand, interviewee C described that employees' responsibilities must be clearly stated. She explained that "*I always say to my department that for example if you approve a payment, you are responsible for that, you should not trust your colleague even if you have worked together a long time, it is your responsibility – to have a healthy way of not trusting everybody."* Interviewees A and B also highlighted that companies must have clearly communicated operational principles for both internal and external processes.

In addition to the previously mentioned factors, interviewee B stressed that internal control must be designed in cooperation with the operative business to ensure that it addresses all relevant risks. Moreover, interviewee A emphasised the importance on understanding where and how fraud can be committed in a specific industry and a specific company. In addition, interviewee B underlined that risks should be continuously identified and assessed. He explained that the sufficiency and effectivity of the controls should be monitored and reviewed based on the continuous risk assessments.

The interviewees also identified challenges with internal control. Interviewee A remarked that opportunity increases the temptation to commit fraud, especially if people know that their actions will not be detected or have any consequences. Interviewee C noted that it is challenging if someone knows exactly how the control processes function and chooses to commit fraud within the control limits. Interviewee A also noted that it is impossible to prevent all internal fraud. In addition, she mentioned that digitalisation has increased the risk of external fraud. In addition to the above-mentioned challenges, the interviewees provided suggestions on how internal control could be improved. Interviewee C described that rotation of personnel could reduce the risk of fraud. She explained that *"in case there are people working a long time with same things and they decide to commit fraud, they probably know exactly how to do it. So, by having rotation, new personnel, you would break up the structures."* Interviewee D argued that automated workflows and processes remove the human subjectivity from the process and would thus decrease the risk of fraud. Interviewee B in turn believed that in many industries a framework which is adapted to the industry and company size could make internal control more effective.

8 Analysis and discussion

In this chapter, the results of the interviews with groups 1 and 2 are compared. The results' relation to the research questions, theory and results from previous studies are also discussed. The fraud triangle theory and the COSO framework for internal control are used as the main theories in the analysis. As described in chapter two, according to the fraud triangle theory, companies can limit the risk of fraud by minimising the opportunity factor with internal control. In addition, as explained in chapter three, the COSO framework is the most cited framework in the field. The analysis is divided into three sections, that is, significance of fraud, use of internal control, and effectiveness and improving of internal control in fraud prevention.

8.1 Significance of fraud

As mentioned in chapter seven, in group 1, the interviewees believed that fraud is a significant risk for companies. They noted, however, that the risk of fraud is affected by several factors, such as a company's size and industry, as well as the levels of incentive and opportunity. This was demonstrated also in the responses in group 2. Two of the interviewees in group 2 believed that the risk of fraud was high due to the large size of the company and number of employees as it is challenging to know what happens throughout the company. The interviewees who believed that risk of fraud is low mentioned that the opportunity to commit fraud was limited due to strong internal control. The responses are in line with the fraud triangle theory presented in chapter two. Biegelman and Bartow (2012) describe that, according to the fraud triangle theory, existing motivation or incentive increase the risk of fraud, whereas limited opportunity decreases the risk. In addition, the findings of Shanmugam et al. (2012) support these views as they found that fraud occurred when opportunity or financial pressure existed.

The interviewees in both groups 1 and 2 mentioned that fraud could cause various types of costs and damage to companies. These responses are in line with the findings of ACFE's (2018a) Report to the Nations, which describes that fraud causes significant costs

to companies. The interviewees in group 2 believed that the internal controls in their companies would limit the costs and damage. This links both to the COSO framework as well as Merna and Al-Thani's (2008) comments on risk management as they both underline that it is impossible to eliminate all risk but that risks can be limited. As mentioned in chapter seven, two of the interviewees in group 2 mentioned that they had had cases of internal fraud. This supports the comments from group 1 about the commonness of fraud in companies.

8.2 Use of internal control

All the interviewees in group 1 described that the complexity of internal control varies between companies depending on a company's size, industry and level of risk. The responses from interviewees in group 2 also illustrate this. The interviewees who work in large companies explained that they have complex and detailed internal control. One of the smaller companies has less complex internal control, while the other smaller company, which operates in a more regulated market, has invested more in internal control. This is also referred to in the COSO framework, as COSO (1994) mention that the framework should be adapted to company specific needs. The COSO framework specifies that large companies require a more formal internal control than smaller companies. This was also reflected in the responses from interviewees in group 1 and interviewees from large companies in group 2. As described in chapter seven, the interviewees mentioned that large companies have thousands of controls and that they must rely on internal control more than smaller companies.

COSO (1994) argues that the framework is adaptable to both large and small companies. The interviewees in group 1 noted, however, that the framework is mainly used in large companies due to its complexity. Moreover, the responses in group 2 indicate that the COSO framework is less applicable to smaller companies as only one interviewee from a large company mentioned that they use the framework. The interviewees' responses support Pickett's (2012) comment that the COSO framework is useful for large companies.

As described in chapter two, Biegelman and Bartow (2012) describe that, according to the fraud triangle theory, companies can limit the risk of fraud by minimising the opportunity factor. They argue that, therefore, internal control is a useful tool for all companies. The interviewees' responses highlight the commonness of internal control. Interviewees in group 1 noted that, although large companies tend to have more complex internal control, there are basic controls that are used in most companies. Interviewees in both groups 1 and 2 described that authorisations, access rights controls and segregation of duties are common controls which companies aim to have. Westhausen (2017) emphasises the importance of internal audit function especially as a fraud detection tool. Moreover, Shanmugam et al. (2012) found in their study that companies which had fraud were missing the internal audit function. It was mentioned in both groups 1 and 2 that monitoring the effectiveness of internal control is essential. Interviewees in group 1 mentioned, however, that internal audit function is mainly used in large companies and companies that operate on a regulated market. The responses from the interviewees in group 2 are in line with the responses from group 1. All three interviewees in group 2 who said that they have internal audit function in use, were either from a large company or a company that operates in a highly regulated insurance market. The fourth interviewee in group 2 noted, however, that internal audit function would be an improvement to their internal control.

Control environment is the first element in the COSO framework and COSO (1994) describe that it sets the ground for the four other elements of the framework. Interviewees in group 1 underlined that the control environment in companies is the basis for the whole internal control process. As described in chapter seven, interviewees noted that sometimes companies' control environment is formally communicated by a code of conduct but often it is referred to as the 'tone at the top'. Interviewees in group 2 described that the importance of internal control is an important variable throughout the control process. Moreover, two of the interviewees in group 2 mentioned that they are regularly tested about the control environment.

8.3 Effectiveness and improving of internal control in fraud prevention

Overall, all the five elements of the COSO framework, that is, control environment, risk assessment, control activities, information and communication, and monitoring, were described in the interviews when the interviewees were asked about effective internal control. Interviewees in group 1 argued that right company culture is an indispensable element for effective internal control. They stressed that underestimating the importance of the control environment can render even the strongest controls ineffective. Moreover, an interviewee in group 2 explained that management's ignorance weakens the internal control process. Although interviewees in group 2 argued that guidelines and instructions alone are ineffective, they underlined that companies' operational principles must be clear both inside and outside companies. Rae and Subramaniam (2008) and Nawawi and Salin's (2018) studies indicate the importance of control environment. Rae and Subramaniam (2008), on the one hand, found that positive corporate ethical environment improves the quality of internal control. Nawawi and Salin (2018), on the other hand, found that company culture and environment within companies affected the likelihood of fraud. Interviewees in both groups 1 and 2 argued that, in addition to the right control environment, companies must clearly assign and communicate responsibility for operations and processes.

Besides having the right control environment, interviewees in both groups argued that the internal control must be properly designed. One interviewee from group 1 explained that companies must ensure that the internal control is adapted to their specific needs and that the controls address all relevant risks. Similarly, one interviewee in group 2 argued that operative business must be included in the design process to ensure that relevant risks are addressed. The COSO framework also remarks that the control activities must be adapted to each company and their risks (COSO, 1994). In addition, another interviewee in group 2 stressed that the people who design and work with internal control must understand where and how fraud can be committed in the company. The COSO framework also advices that, according to the second element of internal control, risk assessment, companies must determine the risks and how they are managed (COSO, 1994). Pickett (2012) in turn explains that if a company identifies the relevant risks, it can also prepare

for them and aim to prevent them. Interviewees in group 1 underscored, however, that it is often difficult for people to believe that fraud could happen in their company or that trusted individuals would commit fraud. When companies struggle to recognise the fraud risk, internal control risks to stay ineffective. This is also reflected in the risk management theory in chapter four as Merna and Al-Thani (2008) explain that companies' unresponsiveness to certain risks can be caused by failure to identify the risk.

The COSO framework underlines that, depending on the operations, entities require different types of controls (COSO, 1994). Although interviewees responses in both groups 1 and 2 indicated that controls vary between companies and departments, interviewees in both groups identified certain controls that are effective regardless of operations or industry. Marshall et al. (2006) explain that controls can be detective or preventive controls. Interviewees in group 1 explained that preventive controls are most effective in the fight against fraud. Moreover, interviewees in group 2 described that controls which allow employees to only do what they are supposed to do in their position are most effective. Two interviewees from large companies in group 2 explained that built-in and automated controls are most effective because they cannot be persuaded or bypassed. Interviewees in both groups emphasised that controls which block unwanted actions are the most effective because employees cannot commit fraud even if they want to. This supports the assumption in the fraud triangle which, according to Biegelman and Bartow (2012), assumes that fraud is prevented when at least one of the triangle's three elements is missing. The built-in and automated controls limit the opportunity to commit fraud. Biegelman and Bartow (2012) argue that out of the three elements companies can best control opportunity. In group 1, one of the interviewees explained that companies must build their internal control so that it aims to eliminate incentive and opportunity. The interviewees described that preventive controls, such as authorisations and access rights controls, effectively limit the opportunity to commit fraud. One interviewee in group 1 and another in group 2 commented that the built-in controls make companies' processes slower. In group 1, the interviewee underlined that companies must remember to assess the cost and benefit relationship when designing the internal control.

Interviewees in group 1 mentioned that ignorance as well as overreliance on imprecise controls and on certain individuals make internal control weak. One interviewee in group 2 also described that internal control is weakened by management's ignorance about design and implementation of internal control. In addition, two other interviewees in group 2 mentioned that controls which are easy to circumvent create an ineffective internal control. Petersen et al. (2018) found in their study that small and mid-sized enterprises tend to use ineffective controls. Moreover, Nawawi and Salin (2018) found in their case study that the company used weak internal controls. Donelson et al. (2017), in turn, found that companies with weaknesses in internal control were more likely to discover financial statement fraud within the company. As the previous studies indicate, only strong and effective internal control helps to prevent fraud. Therefore, it can be concluded that companies must ensure the effectiveness of their internal control. All interviewees in group 1, and one interviewee in group 2, argued that regular monitoring and assessment of the controls ensure the quality of internal control. An interviewee in group 1 explained that, for example, when processes are updated also the controls must be reviewed and updated if necessary. In addition, the interviewee from group 2 underlined that both risks and controls must be assessed regularly. The COSO framework describes that internal control must be monitored with both ongoing monitoring and separate evaluations to ensure the effectiveness of internal control (COSO, 1994). Regarding separate evaluations, one of the interviewees in group 1 argued that regulatory evaluations by a third party could improve effectiveness of internal control. As described in chapter seven, in addition to monitoring the internal control, interviewees in group 2 suggested that rotation of personnel, automated workflows as well as an industry and size adapted internal control framework could improve effectiveness of internal control.

Overall, the interviewees in group 2 believed that their companies have an effective internal control in place. Interviewees in group 1 also described that most companies take internal control seriously and invest a great amount in it. They noted, however, that some companies continue to neglect the internal control and ignore fraud findings. In addition, interviewees in both groups 1 and 2 explained that total elimination of fraud is impossible.

9 Conclusion

This thesis increases the understanding of how companies use internal control to minimise the risk of internal fraud. In addition, it provides insight into how the interviewees perceive the significance of the risk and the effectiveness of different controls. Previous studies show that internal control is an effective tool to prevent internal fraud (Petersen et al., 2018; Puspasari and Suwardi, 2016; Mirinaviciene, 2014; Shanmugam et al., 2012; Barra, 2010; Rae and Subramaniam, 2008). At the same time, studies indicate that some companies use weak internal controls which fail to prevent fraud (Nawawi and Salin, 2018; Petersen et al., 2018; Zakaria et al., 2016). The fraud triangle theory aims to explain why fraud is committed. According to Biegelman and Bartow (2012), the fraud triangle theory was initially introduced by Dr. Cressey. They describe that, according to the fraud triangle, fraud occurs when all three elements of the triangle, that is, motivation, opportunity and rationalisation, are simultaneously present. Regarding internal control, the COSO framework, introduced in 1992, describes that effective internal control consists of the following five elements: control environment, risk assessment, control activities, information and communication, and monitoring (COSO, 1994).

The results of this study indicate that fraud is a significant issue for companies but that it can be limited with strong and effective internal control. The responses show that the use and level of internal control varies between companies. Internal control's level and use is affected by a company's size and industry. In addition, internal control procedures between departments can vary due to different operations. It was also stressed in the interviews that the level of risk affects the internal controls. Companies which face larger threat of fraud are likely to invest more in their internal control. Despite the differences between companies, the interviewees underlined that certain basic controls, such as segregation of duties and access rights controls, are likely to be used in most companies. In addition, the results indicate that effective internal control consists of several elements. The responses show that a company's control environment is a key element in effective internal control. The interviewees stressed that the management must clearly communicate the importance of internal control and that fraud is taken seriously, that is, the 'tone at the top' must be right. According to the results, internal control must also be

adapted to a company's operations and needs. Moreover, companies must understand how their internal control functions and ensure that it addresses all relevant risks. Regarding the controls, results indicate that preventive controls are more effective than detective controls in the fight against fraud. More specifically, automated and built-in controls, which block unwanted actions and allow employees to only access what they are supposed to in their position, were considered the most effective types of controls. According to the results, the final element of effective internal control is regular monitoring and assessment of controls. Moreover, the responses underline that companies must regularly assess that the controls are still up-to-date and address all current risks, as well as ensure that the controls are updated when needed. The results of this study indicate that the quality of internal control could be improved with regular assessment of risks and effectiveness of internal control. Moreover, it was also suggested that regulatory assessments of internal control, by an independent third party, could improve internal control. In addition, increased use of automated workflows and introducing an industry and size adapted internal control framework could improve effectiveness of internal control.

The concepts of credibility and trustworthiness, described in chapter six, were considered during the research process. To increase this study's credibility and trustworthiness, various stakeholders in various positions, both inside and outside companies, were interviewed. Moreover, one of the interviewees checked the analysis of their responses to confirm right interpretation. In addition, the data collection and analysis process are described in detail in chapter six. Despite the above-mentioned actions, the study has limitations. In this study, due to limited resources and time constraints, only one data-gathering method, interviews, was used. In addition, the scope of the study is limited to seven interviews, also because of time constraints. Interviews that are done in person enable the best analysis of the interviewee's responses. Due to geographical and time constraints, and in one case due to large differences in time zones, four interviews were done via Skype for Business and two via email. Especially the analysis of the two interviews done via email are more limited as it was not possible to clarify the questions and ask follow-up questions during the interview. Due to the scope and the research method of this study it is not possible to generalise the results to all companies. Petersen et al. (2018) found in their study that small and medium-sized enterprises often have

ineffective internal control. In addition, interviewees in group 1 noted that small companies often have a more limited internal control due to, for example, limited budget. As none of the interviewees in group 2 are from a small company, the small company perspective is not represented in this study. Therefore, in the future, it could be useful to examine how internal control is implemented and used in small companies and whether the findings of this study also apply to them. In addition, future research could benefit from use of several data-collection methods.

PwC (2018) describe in their publication "Global Economic Crime and Fraud Survey" that internal control can create a false feeling of security. They argue that in order to protect a company, for example from management override, also other measures are required. Moreover, interviewees in groups 1 and 2 described that management override and collusion continue to create problems with internal control. Therefore, future research should explore also other ways to protect companies from internal fraud.

Svensk sammanfattning – Swedish summary

Förhindrande av bedrägerier med intern kontroll

Inledning och problemområde

Företagen har kommit till en bättre insikt om risken för bedrägerier efter olika bedrägeriskandaler, såsom Enronskandalen år 2001. Enligt Association of Certified Fraud Examiners (ACFE, 2018), orsakar bedrägerier förluster vars median uppgår till fem procent av företags intäkter. Det finns både externa och interna bedrägerier. Denna avhandling fokuserar på interna bedrägerier. Även uppskattningen av intern kontroll har ökat under de senaste åren. Intern kontroll kontrollerar verksamheten inom ett företag. Det finns inte någon lagstiftning om hur intern kontroll ska se ut i Europa, utan tillämpningen av intern kontroll varierar mellan olika företag.

Tidigare studier har visat att intern kontroll är ett effektivt verktyg mot interna bedrägerier (Petersen, Bruwer och Le Roux, 2018; Puspasari och Suwardi, 2016; Mirinaviciene, 2014; Shanmugam, Haat och Ali, 2012; Barra, 2010; Rae och Subramaniam, 2008). Samtidigt finns det studier som indikerar att företag använder ineffektiva kontroller (Nawawi och Salin, 2018; Petersen med flera, 2018; Zakaria, Nawawi och Salin, 2016). Donelson, Ege och McInnis (2017) studie visar att företag med svagheter i intern kontroll har större risk för bedrägerier under de följande åren.

Syfte

Syftet med denna avhandling är att öka förståelsen av hur företag använder intern kontroll för att minimera risken för interna bedrägerier i en europeisk kontext. Därtill undersöks olika kontrollers effektivitet. Dessutom betraktas utrymme för förbättring. Forskningsfrågorna i denna avhandling är:

1. *Vilka typer av kontroller används av företag för att förhindra interna bedrägerier?*
2. *Vilka typer av kontroller anses vara mest effektiva för att förhindra interna bedrägerier?*
3. *Hur kan intern kontroll förbättras för att bättre förhindra interna bedrägerier?*

Teori

Denna avhandling bygger på teorier om bedrägerier, intern kontroll och riskhantering. Bedrägeritriangeln är en teori som försöker förklara varför någon begår ett bedrägeri. Biegelman och Bartow (2012) hänvisar till bedrägeritriangeln som introducerades av Dr. Donald Cressey. Biegelman och Bartow förklarar att enligt bedrägeritriangeln är motiv, rationalisering och tillfälle de faktorer som tillsammans leder till bedrägerier. Biegelman och Bartow betonar att alla tre faktorer måste finnas samtidigt. De poängterar att av dessa tre faktorer kan företagen bäst inverka minskande på tillfällen att begå bedrägerier.

Intern kontroll erbjuder ett verktyg för att kontrollera ett företags operationer och minska tillfällen att begå bedrägerier. Företagen kan allmänt välja hur de tillämpar intern kontroll. COSO-ramverket är en modell för intern kontroll. Enligt COSO (1994) är intern kontroll en process som erbjuder rimlig försäkran att företaget når sina mål. COSO-ramverket beskriver att en effektiv intern kontroll består av följande fem komponenter: kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation samt övervakning (COSO 1994).

Metod

Semistrukturerade intervjuer användes som metod i denna avhandling. Enligt Saldaña (2011) är intervjuer en effektiv metod för insamling av data direkt från människor. Totalt gjordes sju intervjuer. De intervjuade indelades i två grupper enligt deras position. Intervjuerna med personer i grupp 1 representerar perspektiv utanför företagen och intervjuer med personer i grupp 2 perspektiv inom företagen. Intervjufrågorna för båda

grupperna testades på förhand i en testintervju med en person som inte deltar i studien. Intervjuerna gjordes på engelska och finska beroende på den intervjuades preferens. Fyra intervjuer skedde via Skype for Business på grund av avstånd och logistik. Dessa intervjuer bandades in och transkriberades. Detsamma gäller en intervju som ägde rum i Belgien. De resterande två intervjuerna utfördes via e-post. Datan från alla sju intervjuer analyserades för att hitta och granska mönster mellan dem.

Resultat och diskussion

Resultaten av denna studie indikerar att bedrägerierna skapar ett signifikant problem för företagen. Å andra sidan signalerar resultaten att risken kan minskas med en stark och effektiv intern kontroll. Intervjuresultaten visar att användningen och nivån av intern kontroll varierar mellan företag beroende på företags storlek, verksamhet samt risknivå. Resultaten indikerar att de företag som lider av större risk för bedrägerier investerar mera i intern kontroll. Resultaten visar dock att det finns grundläggande kontroller, såsom tillträdesrätt-kontroller och uppdelning av arbetsuppgifter, som sannolikt används i nästan alla företag. Dessutom indikerar resultaten att effektiv intern kontroll består av olika delar. De som intervjuades betonade att ledningen måste klart uttrycka betydelsen av intern kontroll och bedrägerierna bör tas på allvar i företaget. Resultaten signalerar också att den interna kontrollen måste vara anpassad efter företagets verksamhet och behov. Dessutom betonades det att företagen måste förstå hur deras interna kontroll fungerar samt säkerställa att den iakttar alla väsentliga risker. Preventiva kontroller ansågs vara mera effektiva än upptäckande kontroller. Mera specifikt ansågs automatiserade och inbyggda kontroller vara den mest effektiva typen av kontroller. Därtill betonades det att företag måste regelbundet övervaka och utvärdera kontrollernas effektivitet. Resultatet av denna studie indikerar att effektiviteten på intern kontroll skulle kunna förbättras med regelbunden monitorering samt utvärdering av risker och intern kontroll. Dessutom poängterades det att obligatorisk utvärdering av intern kontroll utförd av en självständig tredje part skulle kunna förbättra kvaliteten av intern kontroll. Därtill nämndes det att ökad automatisering av processer samt ett ramverk för intern kontroll som är anpassat till storlek och verksamhet skulle kunna effektivera den interna kontrollen. Eftersom endast sju personer intervjuades i denna studie, är det inte möjligt att generalisera resultaten för

alla företag. Ingen av de som intervjuades är från ett litet företag och därför skulle det vara intressant för framtida studier att undersöka ifall resultaten gäller också för små företag. Dessutom skulle det vara intressant att undersöka andra sätt att förhindra interna bedrägerier.

References

Abiola, I. and Oyewole A. T. (2013). *Internal Control System on Fraud Detection: Nigeria Experience.* Journal of Accounting and Finance, 13(5), pp. 141-152.

Accountancy Europe (2019). *Tax Policy Update.* Accountancy Europe, Policy Update. URL: https://www.accountancyeurope.eu/wp-content/uploads/190513_Tax-Policy-Update_Accountancy-Europe.pdf (Read 26/5/2019)

Accountancy Europe (2017). *Auditor's role in fighting financial crime.* Accountancy Europe, Audit & Assurance. URL: https://www.accountancyeurope.eu/wp-content/uploads/180112_Technical-paper-Auditors-role-in-the-fight-against-fraud-corruption-and-money-laundering.pdf (Read 26/5/2019)

ACFE (2018a). *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*. Association of Certified Fraud Examiners.

ACFE (2018b). *What Is Fraud?* URL: http://www.acfe.com/fraud-101.aspx (Read 02/11/2018)

ACFE (2014). *Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study.* Association of Certified Fraud Examiners.

Ahokas, N. (2012). *Yrityksen sisäinen valvonta*. Edita Publishing Oy, Jyväskylä.

Arwinge, O., Eklöv Alander, G. and Nilsson, F. (2013). *Chapter 10, Intern kontroll och ekonomistyrning – två sidor av samma mynt?* Jannesson, E. and Skoog, M. (editors) Perspektiv på ekonomistyrning, pp. 211-231. 1:2 edition, Liber, Stockholm.

Barra, R. A. (2010). *The Impact of Internal Controls and Penalties on Fraud.* Journal of information systems, 24(1), pp. 1-21.

Biegelman, M. and Bartow, J. (2012). *Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance.* Second edition, John Wiley & Sons, Inc., Hoboken, New Jersey.

Brown, R. G. (1962). *Changing audit objectives and techniques.* The Accounting Review, 37(4), pp. 696.

Cassell, C., Buehring, A., Symon, G. and Johnson, P. (2006). *Qualitative methods in management research: an introduction to the themed issue.* Management Decision, 44(2), pp. 161-166.

Childers, D. (2009). *Tapping Into Tips.* Internal Auditor, 66(6), pp. 29-31.

COSO (1994). *Internal Control – Integrated Framework.* Two-Volyme edition, the Committee of Sponsoring Organizations of the Treadway Commission.

Dicksee, L. R. (1905). *Auditing.* Montgomery, R. H. (editor), Ronald Press, New York.

Dimitrijevic, D., Milovanovic, V. and Stancic, V. (2015). *The Role of a Company's Internal Control System in Fraud Prevention.* e-Finanse, 11(3), pp. 34-44

Donelson, D., Ege, M. and McInnis, J. (2017). *Internal Control Weaknesses and Financial Reporting Fraud.* Auditing: A Journal of Practice & Theory, 36(3), pp. 45-69.

Heir, J. R., Dugan, M. T. and Sayers, D. L. (2005). *A century of debate for internal controls and their assessment: a study of reactive evolution.* Accounting History, 10(3), pp. 39-70.

IAASB (2016). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements.* 2016-2017 Edition, Volume I. IFAC.

Lam, J. (2006). *Chapter 1, Managing Risk Across the Enterprise: Challenges and Benefits.* Ong, M. K. (editor) Risk Management, a Modern Perspective, pp. 3-19. Academic Press/Elsevier.

Lincoln, Y. S. and Guba, E. G. (1985). *Naturalistic Inquiry.* Sage Publications, Inc., Beverly Hills, California.

Maijoor, S. (2000). *The Internal Control Explosion.* International Journal of Auditing 4, pp. 101-109.

Marshall, R., Isaac, A. and Ryan, J. (2006). *Chapter 18, Integration of Operational Risk Management and the Sarbanes-Oxley Act Section 404.* Ong, M. K. (editor) Risk Management, a Modern Perspective, pp. 391-412. Academic Press/Elsevier.

Merna, T. and Al-Thani, F. (2008). *Corporate Risk Management.* Second Edition, John Wiley & Sons, Incorporated, Chichester.

Mirinaviciene, S. (2014). *Internal control and fraud prevention: prior research analysis.* Science and Studies of Accounting and Finance: Problems and Perspectives, 9(1), pp. 173-179.

Nawawi, A. and Salin, A. S. A. P. (2018). *Internal control and employees' occupational fraud on expenditure claims.* Journal of Finance Crime, 25(3), pp. 891-906.

Petersen, A., Bruwer, J., and Le Roux, S. (2018). *Occupational fraud risk, internal control initiatives and the sustainability of Small, Medium and Micro Enterprises in a developing country: A Literature Review.* Acta Universitatis Danubius, Œconomica, 14(4), pp. 567-580.

Pickett, K. H. S. (2012). *Fraud smart.* John Wiley & Sons, Incorporated, Chichester.

Puspasari, N. and Suwardi, E. (2016). *The effect of individual morality and internal control on the propensity to commit fraud: evidence from local governments.* Journal of Indonesian Economy and Business 31(2), pp. 208-219.

PwC (2018). *Global Economic Crime and Fraud Survey 2018.* PricewaterhouseCoopers. URL: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf (Read 12/9/2019)

Rae, K. and Subramaniam, N. (2008). *Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud.* Managerial Auditing Journal, 23(2), pp. 104–124.

Saldaña, J. (2011). *Fundamentals of Qualitative Research.* Oxford University Press, USA.

Shanmugam, J., Haat, M. and Ali, A. (2012). *An exploratory study of internal control and fraud prevention measures in SMEs.* International Journal of Business Research and Management, 3(2), pp. 90-99

Sinnett, W. M. (2009). *Does Internal Control Improve Operations And Prevent Fraud?* Financial Executive, 25(10), pp. 32-36.

Spira, L. F. and Page, M. (2003). *Risk management: The reinvention of internal control and the changing role of internal audit.* Accounting, Auditing & Accountability Journal 16(4), pp. 640-661.

Transparency International (2019a). *Anti-corruption glossary.* Transparency International. URL: https://www.transparency.org/glossary (Read 10/5/2019)

Transparency International (2019b). *Western Europe and EU: Stagnating anti-corruption efforts and weakening democratic institutions.* Transparency International. URL: https://www.transparency.org/news/feature/cpi2018-western-europe-eu-regional-analysis (Read 6/4/2019)

Transparency International (2019c). *What is corruption.* Transparency International. URL: https://www.transparency.org/what-is-corruption#what-is-transparency (Read 10/5/2019)

Transparency International (2013). *Whistleblowing in Europe: The time has come to tell a new story.* Transparency International. URL: https://www.transparency.org/news/feature/whistleblowing_in_europe (Read 30/7/2019)

Vähämäki H. (2019). *Turkulaisseura FC Interin pomolle ehdollista vankeutta petoksesta.* Yle Uutiset. URL: https://yle.fi/uutiset/3-10788997 (Read 26/5/2019)

Westhausen, H. (2017). *The escalating relevance of internal auditing as anti-fraud control.* Journal of Financial Crime, 24(2), pp. 322–328.

Wikland, T. (2014). *Intern styrning och kontroll – både lönsamt och säkert.* Third edition, FAR Akademi AB, Stockholm.

Wolfe, D. and Hermanson, D. (2004). *The Fraud Diamond: Considering the Four Elements of Fraud.* CPA Journal, 74(12), pp. 38-42.

World Bank (2014). *Fraud and corruption awareness handbook: A handbook for civil servants involved in public procurement.* World Bank Group, Washington DC. URL: http://documents.worldbank.org/curated/en/309511468156866119/Fraud-and-corruption-awareness-handbook-a-handbook-for-civil-servants-involved-in-public-procurement (Read 15/12/2019)

Zakaria, K. M., Nawawi, A. and Salin, A.S.A.P. (2016). *Internal controls and fraud – empirical evidence from oil and gas company.* Journal of Financial Crime, 23(4), pp. 1154-1168.

Appendix 1 Accompanying letters in English

Group 1

Dear "interviewee's name",

As we discussed in Brussels in the beginning of October, I am writing my master's thesis about preventing fraud through internal control and would like to interview you for my study.

The objective of my study is to increase the understanding of how companies use internal control to prevent fraud. More specifically, I'm interested to hear about your experiences and opinions on what type of controls companies tend to use and what kind of controls you consider most effective for the purpose of preventing fraud. You can find the detailed interview questions attached to this email.

I estimate that the interview will take about one hour, but we can of course adapt the length based on your availability. As we discussed, we could do the interview via Skype for Business call since we are in different countries. I hope we can find a time that suits you for the interview as soon as possible. Preferably, I would like to interview you already during October. Please let me know your availabilities and if you have any questions.

Thank you again for participating in my study!

Kind regards,

Nella Koivisto

Group 2

Dear "interviewee's name"

I am a final year student in Åbo Akademi University, and I am currently writing my master's thesis about preventing fraud through internal control.

The objective of my study is to increase the understanding of how companies use internal control to prevent fraud. More specifically, I'm interested to hear about your experiences and opinions on what type of controls If uses and what kind of controls you consider most

effective for the purpose of preventing fraud. You can find the detailed interview questions attached to this email.

I estimate that the interview will take about one hour, but we can of course adapt the length based on your availability. I would do the interview via call since I live in Belgium.

I hope that you would be willing to participate in my study. Please let me know whether I can interview you and if you have any questions.

Kind regards,

Nella Koivisto

Appendix 2 Accompanying letter in Finnish

Group 2

Hei!

Olen viimeisen vuoden kauppatieteiden opiskelija Åbo Akademissa ja kirjoitan tällä hetkellä Pro gradu tutkielmaani petosten ehkäisystä sisäisen valvonnan avulla. Haastattelen tutkimukseeni taloudenalan asiantuntijoita ja haluaisin haastatella sinua tutkimukseeni.

Tutkimukseni tavoitteena on ymmärtää paremmin, kuinka yritykset käyttävät sisäistä valvontaa petosten ehkäisyyn. Tarkemmin sanottuna, haluaisin kuulla sinun kokemuksiasi ja mielipiteitäsi siitä minkä tyyppisiä kontrolleja yrityksenne käyttää ja minkälaiset kontrollit ovat sinun mielestäsi tehokkaimpia petosten ehkäisyssä. Löydät tarkemmat haastattelukysymykset sähköpostin liitteenä. Arvioni mukaan haastattelu kestäisi noin tunnin mutta voimme totta kai muokata haastattelun kestoa aikataulusi mukaan. Toteuttaisin haastattelun puhelimitse, sillä asun tällä hetkellä Belgiassa.

Ilmoitathan mahdollisimman pian, saisinko haastatella sinua tutkimukseeni ja mikäli sinulla on kysymyksiä.

Mukavaa syksyn jatkoa!

Ystävällisin terveisin,

Nella Koivisto

Appendix 3 Interview guide, group 1

1. What is your role in your organisation?
2. What type of companies do you audit?*
3. How would you define fraud?

   For the following questions, focus on internal fraud, i.e. fraud that occurs within companies (asset misappropriation, corruption and financial statement fraud)
4. How significant do you consider the risk of fraud within companies?
   - How likely is fraud to occur?
   - How much damage would it cause? (e.g. costs or damage to reputation)
   - Are there fields where internal fraud happens more often?
5. How would you define internal control?
6. How do companies implement internal control?
7. Are you familiar with the COSO framework for internal control?
8. According to your experience, is the COSO framework for internal control commonly used in companies?
   - How have companies implemented the COSO framework?
   - How has internal control been implemented in companies in some other way?
9. Can you describe how different activities are controlled within companies? (e.g. code of conduct, internal audit, authorisation, segregation of duties, or access rights controls)
10. How many controls do companies usually have?
11. What types of controls do companies have?
    - What are the most common controls in companies?
12. What do you consider to be most effective types of controls for preventing fraud?
    - Why?
13. What do you consider to be least effective types of controls for preventing fraud?
    - Why?

14. Based on your experience, are there weaknesses in internal control in fraud prevention context?
    - What and Why?
15. In your opinion, how could companies improve their internal control to better prevent fraud?
    - Why?
16. Look at the table 1 of fraud cases in Europe (see page 2). In your opinion, why do some countries have lower number of fraud cases than others?**
    - In your opinion, what role does internal control play for the differences between countries?
    - What other factors could affect the differences between the countries?

Table 1 Number of fraud cases in Western Europe

FIG. 93 **Cases by country in Western Europe**

Country	Number of cases
Austria	4
Belgium	7
Denmark	2
Finland	2
France	4
Germany	16
Greece	22
Iceland	1
Ireland	2
Italy	8
Netherlands	10
Norway	2
Portugal	1
Spain	4
Switzerland	11
United Kingdom	34
Total cases:	**130**

Reference: ACFE 2018a Report to the Nations (pp. 73)

*Not asked from Hilde Blomme

**Only asked from Hilde Blomme

Appendix 4 Interview guide, group 2

Questions in English

1. In which field does your company function?
2. How large is your company?
    - In how many countries does the company operate?
    - How many employees does the company have?
    - What is your company's approximate yearly revenue?
3. What is your role in the company?
4. How would you define fraud?

   For the following questions, focus on internal fraud, i.e. fraud that occurs within companies (asset misappropriation, corruption and financial statement fraud)
5. How significant do you consider the risk of fraud within your company?
    - How likely is fraud to occur?
    - How much damage would it cause? (e.g. costs or damage to reputation)
6. How would you define internal control?
7. Describe your company's internal control
8. Are you familiar with the COSO framework for internal control?
9. Does your company use the COSO framework for internal control?
    - If yes, describe how your company has implemented the COSO framework
    - If no, has your company implemented internal control based on some other framework? Which one and how?
10. Can you describe how activities within the company are controlled? (e.g. code of conduct, internal audit, authorisation, segregation of duties, rotation of personnel or access rights controls)
11. How many controls does your company have?
12. What types of controls does your company have?
13. What do you consider to be most effective types of controls for preventing fraud? Why?

14. What do you consider to be least effective types of controls for preventing fraud? Why?
15. In your opinion, how could companies improve internal control to better prevent fraud?
    - Why?

Questions in Finnish

1. Millä alalla yrityksenne toimii?
2. Kuinka suuri yrityksenne on?
    a. Kuinka monessa maassa toimitte?
    b. Kuinka monta työntekijää yrityksessänne on?
    c. Kuinka suuri yrityksenne keskimääräinen vuosittainen liikevaihto on?
3. Mikä on roolisi yrityksessänne?
4. Miten määrittelisit käsitteen petos?

   Seuraavissa kysymyksissä sanalla petos viitataan yritysten sisäisiin petoksiin (yrityksen varojen väärinkäyttö, korruptio sekä petos kirjanpidossa ja tilinpäätöksessä)
5. Kuinka merkittävä riski petos on mielestäsi yrityksellenne?
    a. Kuinka todennäköisesti yrityksessänne voisi tapahtua petos?
    b. Kuinka paljon vahinkoa petos aiheuttaisi yrityksellenne? (esimerkiksi kustannuksia tai vahinkoa maineelle)
6. Miten määrittelisit käsitteen sisäinen valvonta?
7. Kuvaile yrityksenne sisäistä valvontaa
8. Onko COSOn sisäisen valvonnan ohjekehys (COSO framework for internal control) sinulle tuttu?
9. Käyttääkö yrityksenne COSOn sisäisen valvonnan ohjekehystä?
    a. Jos kyllä, miten yrityksenne käytännössä käyttää COSOn sisäisen valvonnan ohjekehystä?
    b. Jos ei, käyttääkö yrityksenne jotakin toista sisäisen valvonnan ohjekehystä? Mitä ja miten?

10. Kuvaile kuinka yrityksenne kontrolloi erilaisia toimintoja käytännössä (esimerkiksi code of conduct, sisäinen tarkastus, valtuutus, vastuiden erottelu, työnkierto tai pääsyoikeus kontrollit)
11. Kuinka monta kontrollia yrityksellänne on?
12. Minkä tyyppisiä kontrolleja yrityksellänne on?
13. Minkä tyyppiset kontrollit ovat mielestäsi tehokkaimpia petosten ehkäisyssä?
    a. Miksi?
14. Minkä tyyppiset kontrollit ovat mielestäsi vähiten tehokkaita petosten ehkäisyssä?
    a. Miksi?
15. Miten yritykset voisivat mielestäsi parantaa sisäisen valvonnan tehokkuutta petosten ehkäisyssä?
    a. Miksi?

Appendix 5 Interviewee and interview details

Interview group	Interviewee title	Nationality	Role	Industry of the audited companies (group 1) / Industry (group 2)	Size of the company: countries/employees/ revenue	Interview language	Interview date	Interview duration (min)	Interview location
Group 1	Hilde Blomme	Belgian	Deputy CEO of Accountancy Europe, also CPA in Belgium, the UK and the US	N/A	N/A	English	21 October 2019	60	Belgium
Group 1	Myles Thompson	British	Technical audit partner KPMG UK	Especially manufacuring, chemical and pharmaceutical companies	N/A	English	22 October 2019	40	Online interview
Group 1	Partner A	German	Professional practice director	Large multinational companies	N/A	English	24 October 2019	30	Online interview
Group 2	Interviewee A	Finnish	Financial manager	Building and industrial services	6/2 500/EUR 350M	Finnish	25 October 2019	35	Online interview
Group 2	Interviewee B	Finnish	Controller	Insurance	1/25/EUR 17M	Finnish	28 October 2019	N/A	Email
Group 2	Interviewee C	Finnish	Head of cash and credit managent	Insurance	7/6 700/ EUR 4 300M	English	29 October 2019	40	Online interview
Group 2	Interviewee D	Finnish	CFO	Education	3/120/EUR 22M	English	8 November 2019	N/A	Email