The role of internal accounting controls in preventing and detecting financial statement fraud: a qualitative Dutch study

Tijmen Lintsen
Thesis, Master of Science, Business Administration
University of Twente, Enschede, the Netherlands

Abstract

This thesis investigates the effect internal control systems have on financial statement fraud in the Netherlands. It aims to provide insights on why internal control systems failed to prevent fraud and how it can prevent fraud in the future. Multiple case studies of major Dutch fraud cases are analyzed using the CRIME model developed by Rezaee (2005). In addition to that interviews are held with six employees working at a major accountancy firm. Results show that the most important dangers to internal control systems are management override and collusion. The risk of management override can be minimized by proper segregation of duties. The risk of collusion can be minimized by investing in soft controls. An effective internal control system requires a combination of the right hard controls and soft controls.

Acknowledgements

I would first like to thank my thesis advisor Dr. S.A.G. Essa of the Faculty of Behavioral, Management and Social Sciences at University of Twente. Prof. Essa always responded quickly when I ran into a trouble spot or had a question about my research or writing. Writing this thesis proved difficult but he provided constructive feedback whenever I needed it.

I would also like to thank the interviewees for their participation in this study. Without their passionate participation and input, the questions could not have been answered.

I would also like to acknowledge Tom Bosch as advisor from the company, I am gratefully indebted to him for his very valuable comments on this thesis.

Finally, I must express my very profound gratitude to my parents and to my girlfriend for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Tijmen Lintsen

Table of Contents

1 Introduction

The association of certified fraud examiners (2016) report that on average organizations lose 5% of their revenues to fraud each year. PriceWaterhouseCoopers (2011) reports one of the most challenging problems for business is fraud, it states that 50% of worldwide organizations has been subject to fraud in the last two years. In response to this crisis it is important that internal accounting controls, and strategies for preventing and detecting financial statement fraud are improved (Mohamed, 2013). KPMG (2007) states that these strategies need to be incorporated in all levels of the organization and supported by everyone including the board of directors, executives, audit committee and accountants. As of today discussions have focused on the importance of prevention and detection strategies that can be used to reduce the chance of financial statement fraud. Although many previous research has not examined the actual practices of financial statement fraud controls, they do suggest that improvement in those controls is required (Mohamed, 2013).

Financial statement fraud is defined as by the association of certified fraud examiners as: *"The intentional, deliberate, misstatement or omission of material facts, or accounting data which is misleading and, when considered with all the information made available, would cause the reader to change or alter his or her judgment or decision" (p.2).*

To explain financial statement fraud the fraud triangle was developed. It requires three variables in order for someone to commit financial statement fraud: pressure, motivation and opportunity. An effective internal control system attempts to identify and reduce opportunities. When speaking of the internal control system one means the formal mechanism of balances and checks that auditors test as part of the assurance they provide on financial statements.

Many strategies such as internal audit departments, knowledgeable supervisory board or tone at the top aimed at improving internal control systems are recommended by literature (KPMG, 2005; PWC, 2007; Rejda, 2008; Vaughan, 1997; Wells, 2002; Smith et al.; 2002). Despite extensive literature on fraud prevention there have been many major fraud cases in the Netherlands. The following cases will be studied: Imtech, Ahold, Delta Lloyd, SBM Offshore, Heineken, Innoconcepts, SNS Reaal, Vestia, LCI computer and KPNQwest

In this research I provide an answer to the research question:

"Why internal control systems failed to prevent financial statement fraud in Dutch organizations?"

International literature offers the following explanations. Management override is listed as the Achilles heel of fraud prevention by the AICFE (2005). Because management is responsible for the design, implementation and maintenance of internal control. Therefore otherwise effective internal control system cannot be relied upon to prevent financial statement fraud committed by top management (AICFE, 2005) (Dorminey et al. 2012) (Pfister, 2009). Kinney (2000) shows in his paper that expenditure on internal control has a quality optimum. The total costs are calculated by a sum of decision error cost, asset loss cost, residual risks and costs of internal control. Past a certain point investing in internal control is ineffective because the costs exceed the benefits, top management is responsible for finding this point (Kinney, 2000). Some organizations might not have the financial means to maintain an effective internal control system in the ever changing business environment (Dorminey et al. 2012). While other organizations might overdue spending on internal control leading to an ineffective system (Pfister, 2009). When employees constantly work with internal control they familiarize with the systems strengths and weaknesses. This enables them to circumvent internal control by exploiting the systems weaknesses (Dorminey et al. 2012). Collusion is when two or more people cooperate to circumvent internal controls for plethora of reasons. A report by AICPA (2005) shows that when collusion is present internal controls are generally ineffective. This paper aims to explain the role of internal accounting controls in preventing financial statement fraud in Dutch organizations. This leads to the following research questions:

1. How was financial statement fraud comitted at major Dutch organizations?
2. How do Dutch organizations create effective internal control systems?
3. What dangers are there to internal control systems in Dutch organizations?

To answer the previous questions this research will combine multiple case studies with expert interviews. Dutch financial statement fraud cases will be analyzed using the CRIME model. This will provide an answer as how the fraud was committed and what internal controls could have prevented the fraud or detected it earlier. In addition to the case studies interviews are held with

experts in the field of fraud prevention, this will in depth information on internal control systems and the dangers they face.

The ethical implications of this study that have been considered are as follows: First, the need to obtain the consent for interviews with experts from KPMG. Second, the research is concerned with the confidentiality and sensitivity of the information from all organizations that might come forward in the interviews.

This research provides some evidence consistent with international literature (AICFE, 2005; Dorminey et al., 2012; Pfister, 2009; AICPA, 2005) who identify management override and collusion as the largest dangers to internal control systems. In addition some evidence is found for the role of financial distress in increasing risk of financial statement fraud (Krishnan, 2005). Inconsistent with international literature this research provides evidence that familiarization or the gain/loss principle are not responsible for weaker internal control systems, but instead are consequences of a weak internal control system (Kinney, 2000; Dorminey, Fleming, Kranacher, & Riley, 2012). In addition the case study provides evidence that top management is usually responsible for committing financial statement fraud, using false invoices to hide it. Self-enrichment is the primary incentive for the fraudsters. In every case some form of management override is partly responsible for the failure of internal control, however management override is never the sole reason. Poor segregation of duties, fraud culture and/or collusion usually complement management override. Last interviewees described efficient internal control systems as: Best practice in creating an efficient internal control system is a good combination between soft and hard controls. Without proper soft controls, hard controls are inefficient. Other best practices are risk analysis, and having a good accountant. The most important hard control is segregation of duties. Other important hard controls are visibility of controls and the four eyes principle. Last it is important to check whether controls are actually complied with, and done properly. In order to increase internal control efficiency risk analysis is very important, organizations need to cover the right organization specific risks with the right controls. Automation of controls is an upcoming trend to further increase efficiency. Trends in fraud prevention strategy are IT controls. This works two ways, IT systems are becoming more complex thus requiring more controls. And IT systems offer more in the form of fraud detection by for example automating data analysis discovering anomalies. Data analysis is named to be the most important fraud detection tool, accountants look for anything out of the ordinary. An

example is a booking out office hours. Last efficient internal control systems are reported to be vital for the continuation of the organization.

Validity of this research has been improved in two ways. First ten case studies have been done, this makes sure results are not on a one time basis and generalizable to organizations in the Netherlands. In addition to that six interviews are held with experts working in the field of accountancy. These six interviewees have worked for a large number of clients ensuring the validity of the results.

Until now most research on internal control systems and fraud prevention has been done internationally. This thesis contributes to the financial statement fraud literature by explaining the dangers to internal control systems in the Dutch environment. And by providing a view on internal control systems from the Dutch accountancy profession.

Section two provides background on the financial statement fraud, reviews the prior literature, and develops our hypotheses. Section three describes the methods used for this research. In section four the results will be described. Section five contains the discussion and conclusion. Section 6 describes the references. And last in section seven the appendices will be given.

2 Literature Review

A lot of research on the topic of financial statement fraud has been done (e.g., Albrecht, Howe & Romney, 1984; Beasley & Hermanson, 2010; Gullkvist & Jokipii, 2013; Jones, 2011; Rezaee & Riley, 2011; Ernst & Young, 2003; KPMG, 2012; PWC, 2011; The association of certified fraud examiners, 2012) have all shown tremendous costs of financial statement fraud, although their actual numbers differ. The literature review will be structured as follows: In paragraph 2.1 existing research on financial statement fraud will be discussed. Then the evolution of the fraud triangle, a theory that explains the existence of financial statement fraud will be reviewed (Cressey, 1953; Dorminey, Fleming, Kranacher & Riley, 2012). After that accounting internal control will be explained and last the relation between these three variables will be discussed.

2.1 Financial statement fraud

2.1.1 Creative accounting

Creative accounting is when managers use the freedom given to them by accounting rules and regulations, to make their organizations standing appear better than it actually is. When managers go further and break the rules and procedures creative accounting becomes financial statement fraud (Jones, 2011). One could say that one leads to the other. Creative accounting is so common that Yadav claims it happens in every company (2013). One of the first books written on creative accounting was written by Griffiths (1986). In his book Griffiths claimed that every company in the United Kingdom was using creative accounting too improve its profits and called it the biggest con trick since the Trojan horse. In general one can state that there are two views on creative accounting, a wide one that includes fraud (Mulford & Comiskey, 2002) and a narrow one that views creative accounting as using the flexibility in accounting regulations to legally serve their own interest (Jones, 2011). In this thesis the wider definition of creative accounting is used as given by Mulford & Comiskey (2002) as follows: *"Any and all steps used to play the financial numbers game, including the aggressive choice and application of accounting principles, both within and beyond the boundaries of generally accepted accounting principles, and fraudulent financial reporting. Also included are steps taken toward earnings management and income smoothing (p.15)."*

2.1.2 The definition of financial statement fraud

When creative accounting breaks the rules it becomes financial statement fraud, which is defined by Beasley, Carcello & Hermanson (1999) as: *"Intentional material misstatement of financial statement or financial disclosures or the perpetration for an illegal act that has a material direct effect on the financial statements or financial disclosures." (p.3).*

The association of certified fraud examiners provide a slightly different definition: *"The intentional, deliberate, misstatement or omission of material facts, or accounting data which is misleading and, when considered with all the information made available, would cause the reader to change or alter his or her judgment or decision" (p.2).*

The difference lies in the description of a material effect. The association of certified fraud examiners describes this as an effect that causes the reader to change or alter his or her judgment or decision.

Fraud against a company can be committed both internally and externally. Internal fraud or also called occupational fraud is defined by the association of certified fraud examiners as: *"The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets." (p.2).* Occupational fraud is when an employee uses his position for personal enrichment by deliberately misusing the organizations resources. There are three ways one can commit occupational fraud: (1) asset misappropriation (2) corruption and (3) financial statement fraud. Asset misappropriation is when an individual steals resources. Corruption is when an individual misuses his influence in business transactions to further his own gain, for example by accepting bribes (The Association of Certified Fraud Examiners, 2016). Financial statement fraud can be split in two types. The first type is when organizations uses accounting practices that are not allowed by the rules and regulations. With this type it is often difficult to distinguish between fraud and creative accounting, because regulation agencies are unsure where to draw the line (Jones, 2011). The second type of fraud is when organizations record fictitious transactions in their books (Jones, 2011). For example in the Satyam fraud, around 1 billion in cash was admitted to be nonexistent by the current CEO. Golden, Skalak & Clayton (2006) stated five different basic elements of financial statement fraud in their research: (1) A falsified representation of material nature, (2) Knowing that the representation is false, (3) Victim relies on the falsified representation and (4) Financial damages for the victim, and financial gain for the fraudster.

2.1.3 The cost of financial statement fraud

Financial damages to the victims were estimated by the Association of Certified Fraud Examiners (2016) who report that five percent of revenues are lost to fraud by the average organization each year. The total revenue in the Netherlands was estimated to be €676 billion by the Centraal Planbureau Statistiek (CBS) in 2015. This means that an estimated total sum of €33 billion was lost to fraud in the Netherlands in 2015. However it is very difficult to determine the true costs of financial statement fraud. This has multiple reasons. First of all not all fraud is detected and when fraud is detected it is not always reported. In addition to this not all costs are direct costs, some costs like loss of goodwill are indirect and hard to measure. Last the direct costs are often downsized by fraudsters in legal cases. Therefore actual costs of financial statement fraud are likely to be even higher (Rezaee & Riley, 2011).

The actual costs of financial statement fraud have been analyzed by the association of certified fraud examiners (2016) who estimated the average loss of financial statement fraud to be $2.7 million per case. For a total of $6.3 billion over 2400 cases in the study. In 83% of the cases the fraud contained misappropriation, corruption occurred in 35.4% of cases and financial statement fraud occurred in 10% of the cases. This might make financial statement fraud seem small compared to the other two. However the median value of financial statement fraud is $975,000. In contrast the median value of asset misappropriation is $125.000 and that of corruption is $200.000. The median value is chosen because the outliers make averages skewed towards one side (The Association of Certified Fraud Examiners, 2016). The study by ACFE does not include indirect costs, such as harm to the organizations reputation or loss of relations with stakeholders. Instead it measures direct costs like the money that was stolen or fines.

In addition, this $6.3 billion total only reflects direct losses suffered by the victim organizations; it does not include indirect costs, such as reputational harm or loss of stakeholder relationships, so the true total loss represented by these cases is likely much higher

Another reason to research financial statement fraud and internal controls in particular is the following finding: *“When fraud was uncovered through active detection methods, such as surveillance and monitoring or account reconciliation, the median loss and median duration of the schemes were lower than when the schemes were detected through passive methods, such as notification by police or by accidental discovery.” (The Association of Certified Fraud Examiners, 2016, p. 4).*

The research also shows that the presence of anti-fraud controls correlate with lower fraud losses and faster detection of fraud. When the association of certified fraud examiners compared organizations that have those controls in place, and those that don't it was shown that fraud losses were 14,4%-54% lower and frauds were detected 33.3-50% faster (The Association of Certified Fraud Examiners, 2016). Last the report reported that lack of internal controls (29.3% of the cases) and override of internal controls (20% of the cases) were the most prominent organizational weaknesses (The Association of Certified Fraud Examiners, 2016).

2.1.4 The different parties involved in financial statement fraud

Because of the high cost of financial statement fraud many different parties are involved: Managers, investment analysts, regulators, auditors, shareholders, merchant banks, other users and legal authorities (Rezaee & Riley, 2011). Managers have the most important role in financial statement fraud, managers have the most to gain from financial statement fraud and it's generally management that actually commit the crime (Rezaee & Riley, 2011). Cressey (1983) described that there are three conditions that have to be met in order for a manager to commit fraud: Opportunity, knowledge, and pressure. Examples of personal incentives for managers to commit financial statement fraud described by Jones (2011) are lifestyle, gambling or debt. Managers might start with creative accounting and then move on to committing fraud when creative accounting does not give the right results (Jones, 2011). Investment analysts are people that value organizations. In order to be able to do this they need to spot creative accounting or fraud and adjust for it, however research in Germany shows that they fail to do this more often than not (Breton & Taffler, 2001). Regulators are institutions that set rules to control creative accounting and prevent fraud. Rules reduce the freedom of managers, which may reduce the information effectiveness. An example of this is the case of medicine manufacturers as they cannot properly capitalize their R&D efforts due to regulation (Rezaee & Riley, 2011). Auditors are the people who are responsible for checking the accounts to make sure that they provide a fair presentation of the results (Jones, 2011). One of the main problems of auditors is to maintain their independence, as the management they are checking is also paying them (Jones, 2011). Shareholders are people that hold a stocks in the company. They can profit from fraud on the short term as share price might rise when it should fall. However on the long term shareholders will always lose as it is the management that reaps any profit, whereas the shareholders walk the risk of losing their investment (Rezaee & Riley, 2011) (Jones, 2011). Merchant banks is the

group responsible for setting up accounting schemes. Other users are groups that do not fit in any of the categories e.g. employees. This group is generally harmed by financial statement fraud. And lastly in the case of detected financial statement fraud legal authorities will deal with the perpetrators (Jones, 2011). Managers and auditors will have most to do with internal controls. Management is responsible for putting the right controls in place, whereas auditors should evaluate if this has been done. The failure of internal controls could be related to these two groups. Figure 1 on the next page provides a visual representation of all groups.

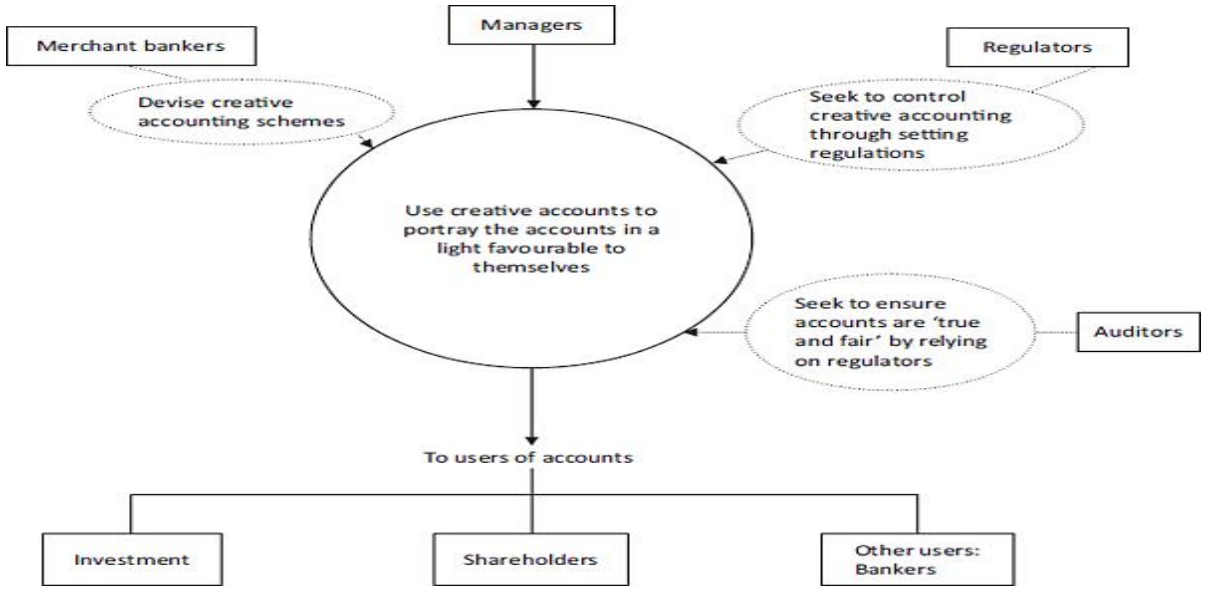

Figure 1. Different parties involved in financial statement fraud (Jones, 2011).

Management is generally the party that commits financial statements fraud. Some motivations for committing financial statement fraud are: Obtaining credit, stock value, hiding bad performance, hiding fake business transactions and resolving financial distress. Personal incentives for management to engage in financial statement fraud like increased compensation, improving value of personal stock, stealing the company's assets, getting a promotion (Rezaee & Riley, 2011). Other authors identify very similar reasons some examples are meet company goals and objectives, meet financing covenants, receive bonuses obtain new financing, attract new investment capital, increase earnings per share, decrease negative market perception (Robertson, 2000). People are more likely to commit financial statement fraud when there is a strong motive, opportunity and when the scheme is considered to be acceptable (Rezaee & Riley, 2011).

2.1.5 Financial statement fraud schemes

Gao & Srivastava (2011) classify fraud into accounting schemes and evidence schemes. Accounting schemes are those methods that are used to commit to fraud, and evidence schemes are used to cover it up (Gao & Srivastava, 2011). The association of certified fraud examiners (1996) has divided fraud into three groups: Asset misappropriation, fraudulent statements and bribery and corruption. Misappropriation is the easiest way to commit fraud, and is defined as stealing inventory, cash or other assets from the company (ACFE, 1996). Fraudulent statements can be created by creating fictitious sales, cash or inventory which distort the balance sheet. Beasley & Hermanson (2010) divide financial statement fraud schemes in three groups: improper revenue recognition (50%), overstatement of assets (50%) and other fraud schemes (58%). KPMG (2007) recognizes the following ways of committing financial statement fraud: (1) fraudulent financial reporting, (2) misappropriation of assets, (3) revenue or assets gained by fraudulent acts, (4) expense incurred from fraud and (5) other misconduct like insider trading. The committee of sponsoring organizations (COSO) (1999) state in a report that fifty percent of studied fraud cases are overstated revenues by recognizing sales too early or creating fictitious sales, fifty percent are overstatement of assets, eighteen percent are understatement expenses and liabilities, twelve percent are misappropriation of assets, eight percent are improper disclosures and twenty percent are defined as other fraud schemes. Examples of common fraud schemes are: (1) improper cutoff of transactions, (2) inadequate disclosure, (3) improper deferral of costs, (4) improper asset valuations, (5) improper revenue recognition, (6) illegimate sales transactions, (7) side arrangements, (8) bill and hold sales transactions and (9) timing of revenue recognition. The first is improper cutoff of transactions at the end of a reporting period. This usually happens with interim statements. Second is inadequate disclosure which is a managers choice not to disclose financial information in the footnotes. Third is improper deferral of costs, which is failure to disclose warranty costs. The fourth example is improper asset valuations often this is recording fictious inventory, accounts receivable or fixed assets. Fifth is improper revenue recognition, for example inappropriate use of percentage of completion method for contracts. Sixth is illegimate sales transactions, often ficitious sales with fake customers. Seventh are side arrangements which often involve sales with conditions that may have a result in the overstatement of assets. Eight is bill and hold sales transactions, which are transactions that take place when the customer buys the goods but the seller retains possesion until the customer requests shipement, in this case the

company can recognize sales too early. And last timing of revenue recognition usually consists of too early recognition to overstate sales that are typically fictious (Rezaee & Riley, 2011).

2.1.6 Financial statement fraud prevention

In order to reduce the chance of successful financial statement fraud schemes Rezaee & Riley (2011) advice organizations to put prevention, detection and correction mechanisms in place. Important elements of prevention are: (1) board of directors, (2) audit committee, (3) diligent management and (4) internal audit. Important elements of detection are: (1) internal controls, (2) responsible legal counsel, (3) external audit and (4) external oversight procedures. Correction methods are centered on restatement of fraudulent financial statements and new strategies to regain public confidence after a fraud (Rezaee & Riley, 2011). Corporate governance is responsible for reducing the effects of pressure, opportunity and rationalization as discussed in the next section. To do this the following elements can be used (1) code of conduct, (2) vigilant board of directors and audit committee, (3) effective internal control structure, (4) internal audit function and (5) external audit. While prevention of financial statement fraud is the best strategy for ensuring the quality of financial reports it's too expensive and hardly possible to prevent all frauds. Therefore internal and external auditors should detect fraud as soon as possible. Detecting financial statement fraud can be done by identifying red flags. Red flags are indicators of financial statement fraud. Appendix A provides an extensive list of financial statement fraud red flags, some examples will be given in this paragraph. One such example is observing management life style for example spending more money than one should be able to considering ones salary. Business red flags are aimed at identifying managers who attempt to overcome difficulties with obtaining equity or loans by committing financial statement fraud to make the organization look better. Examples of red flags include: Weak corporate governance, absence of oversight board / audit committee, weak internal controls, emphasis on earnings, domination by one person or group, aggressive attitude on meeting goals, profit is larger than industry profit, unusual related party transactions, high turnover accounting personal and last trouble with other auditors (Rezaee & Riley, 2011). Rezaee & Riley (2011) recommend organizations to employ the following strategies to reduce the risk of financial statement fraud: *"Establishing a responsible corporate governance, vigilant board of directors and audit committee, diligent management, as well as adequate and effective internal audit functions. Using an alert, skeptical external audit function, responsible legal counsel, adequate and effective internal control*

structure, and external regulatory procedures. Implementing appropriate corporate strategies for correction of the committed financial statement fraud, elimination of the probability of its future occurrences, and restatement of the confidence in the financial statement process. (p.87)".

2.1.7 Anti-fraud rules and regulation

In the United States of America a wave of fraud scandals resulted in a drop in investor confidence (Cohen, Dey, & Lys, 2007). These fraud cases were highly public and ultimately were responsible for the passage of the Sarbanes Oxley Act (SOX, July 30, 2002). The law contains eleven sections about corporate board responsibilities, criminal penalties and requires the Securities and Exchange Commission (SEC) to implement new rules and requirements on how to comply with the law. The SOX is also responsible for creating the Public Company Accounting Oversight Board (PCAOB). The board is responsible for overseeing, regulating, inspecting and disciplining accounting companies that are auditors of public organizations. The act is also about things like corporate governance, internal control and financial disclosure (Kimmel, Weygandth, & Kieso, 2011).

In the Netherlands there are two forms of regulation. Self-regulation and regulation by law. Self-regulation is in the form of the "Nederlandse Corporate Governance Code". This is the replacement of the "Tabaksblad code" that was the Dutch version of the American SOX regulation. The Code contains principles and best practices that regulate the relationship between the board, the supervisory board and the shareholders. The principles and best practices are aimed towards long term value creation, risk management, effective management and supervision, rewards and the relationship with shareholders and stakeholders. The principles are a package of broadly accepted general beliefs about good corporate Governance. The principles are elaborated in best practice provisions. These provisions contain standards for the behavior of directors, supervisory directors and shareholders. When companies want to abstain from the rules they have to explain why in their statements (Monitoring Commissie, 2016). The Corporate Governance code is imbedded in the Dutch "Burgerlijk Wetboek" in article 2:141. Other examples of law are "Wet Bestuur en Toezicht" which gives a clear view of hard controls in an organization. And "Huis voor Klokkenluiders" which is aimed at protecting whistleblowers (De Kort & Elst van der, 2014).

2.2 The fraud triangle

2.2.1 The original fraud triangle

The fraud triangle theory states that there are three variables present in every fraud: (1) motive, (2) rationalization and (3) opportunity (Cressey & Sutherland, 1992).

Figure 2. The fraud triangle (Dorminey et al., 2012)

The foundations for the fraud triangle are laid out by Edwin H. Sutherland in 1940 when he invented the term white-collar crime. Before that research had been focused on street- and violent crime, which are usually committed out of poverty. White-collar crimes are usually not committed out of poverty. Sutherland identified three additional ways in which white collar criminals are different from street criminals. First because white collar crimes are generally committed by people with high social standing that are admired and feared by members of the society, which leads to lower punishments. Second because of the status there is lower trust on the normal justice system, with fines or probation often being given to fraudsters. Third and last white-collar crimes are less obvious because the consequences are faced over a longer period, and generally hit more people that carry the consequences together (Sutherland, 1940). While researching white-collar offenders Sutherland was mentoring Cressey. Cressey (1950) identified three general characteristics all fraudsters have when interview white collar criminals. The first characteristic is a non-shareable financial problem, the second is knowledge of the workings of an organization and the third is the ability to make the crime seem right in the perpetrators own eyes (Cressey, 1950). Later Cressey refined these three characteristics into three criteria that must be there in order for someone to commit financial statement fraud: perceived pressure,

perceived opportunity and rationalization. This is the first form of the fraud triangle (Cressey, 1953). Perceived pressure that originates from a non-shareable financial problem is the motivation for the fraud. A fraudster might think a problem is not shareable because of social stigma (extreme disapproval of a person/group) coming with the problem or because of their ego. Perceived opportunity is the ability to act and to do so without risking being detected. The last part of the fraud triangle is rationalization which is the need for fraudsters to be able to justify the action before they commit their first fraud (Dorminey, Fleming, Kranacher, & Riley, 2012). The fraud triangle is an efficient model that serves as help to understanding fraud (Dorminey et al, 2012). For example the association of certified fraud examiners and almost every other auditing textbook covers the fraud triangle (ACFE, 2009). Next to this there is also research supporting evidence for existence of the fraud triangle conditions in fraud cases (Bell & Carcello, 2000) (Hogan, Rezaee, Riley, & Velury, 2008). However there are cases in which the fraud triangle is does not fully explain the fraud. An example is the case of commercial bribery in which multiple people are needed to commit fraud. It is unlikely that all those people have a non-shareable financial need (Dorminey et al, 2012). For those cases critics have developed adaptations for the fraud triangle which will be discussed next.

2.2.2 The fraud triangle of action

The triangle of fraud action consists of the act, concealment and conversion. Whereas the triangle of fraud primarily focusses on the fraudster, the triangle of fraud action focusses on the act. The act means the methodology of the fraud. Concealment means hiding the fraud. And conversion means turning the stolen goods into something useful for the fraudster, for example laundering money. The triangle of fraud action is primarily used to provide evidence for fraud. Where the fraud triangle tries to provide an answer as to why someone commits fraud. Anti-fraud professionals can use the triangle of fraud action to set control points where fraud may be prevented or detected (Albrecht, 2006).

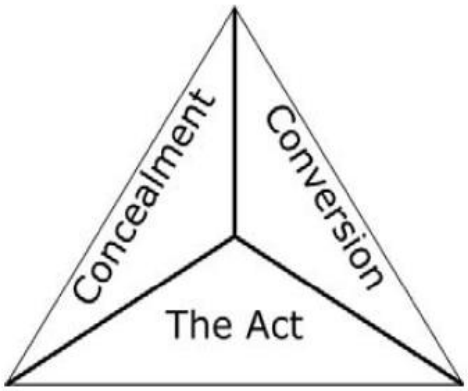

Figure 3. The fraud triangle of action (Dorminey et al., 2012)

2.2.3 The fraud scale

The fraud scale also uses pressure and opportunity from the fraud triangle but replaces rationalization with personal integrity. The fraud scale was created by Albrecht, Howe & Romney in their book in 1984. It was developed by analyzing 212 fraud cases in the early 80's. The data came from internal auditors. Inspecting integrity over rationalization has the advantage that integrity can actually be inferred from past behavior as well as current decision making process. Persons that have high integrity are less likely to rationalize crimes (Albrecht, Howe, & Romney, 1984).

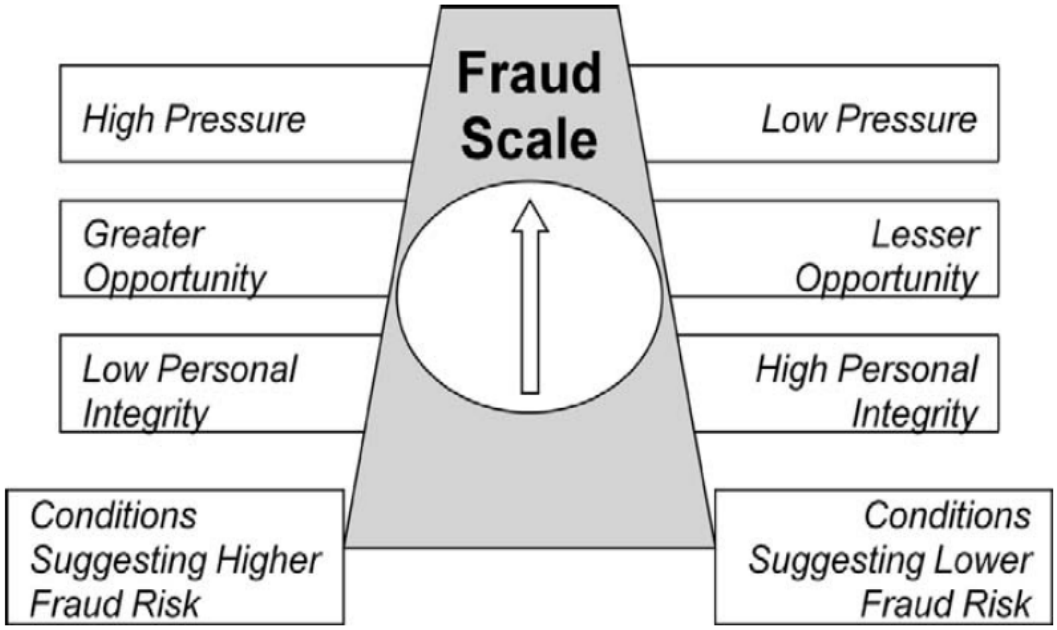

Figure 4. The fraud scale (Dorminey et al., 2012)

2.2.4 Money, ideology, coercion and ego (M.I.C.E.)

The M.I.C.E theory changes the pressure part of the fraud triangle into money, ideology, coercion and ego pressures because not every fraud case has the component of a non-shareable financial problem. Therefore motivations by fraudsters to commit fraud are better explained by the M.I.C.E. acronym according to some authors (Kranacher, Riley, & Wells, 2011). Money and ego are self-explanatory and most common forms of pressure. Ideology is when someone commits fraud out of ideology, an example is when someone thinks he pays enough taxes or that taxes are unconstitutional. A scarier example is when someone commits fraud to raise money for terrorists' attacks. Last someone may commit fraud because he or she is unwilling but coerced to do it.

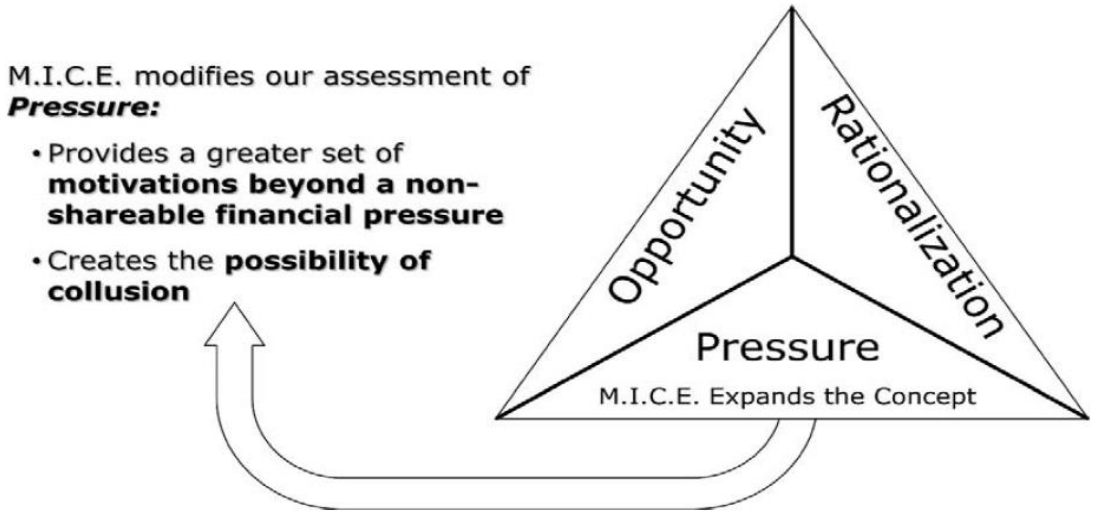

Figure 5. The impact of M.I.C.E on the fraud triangle (Dorminey et al., 2012)

2.2.5 The fraud diamond

Wolfe & Hermanson (2004) add capabilities to the fraud triangle, effectively creating the fraud diamond. The idea is that without the capabilities to exploit weaknesses in the control system no fraud can possibly occur. The authors explain capabilities as the possibility someone has to detect the door, whereas rationalization, opportunity and pressure is what allows someone to actually open the door. Without the ability to recognize an opportunity in an organization defenses there will be no fraud. Therefore capability is the ability to recognize an opportunity

(Wolfe & Hermanson, 2004). The author identify the traits someone needs to commit long large scale fraud as intelligence, ego, position and the ability to cope with stress for long periods time. Capabilities modifies the opportunity concept by limiting it to a small set of individuals having the skill to commit long term large scale fraud.

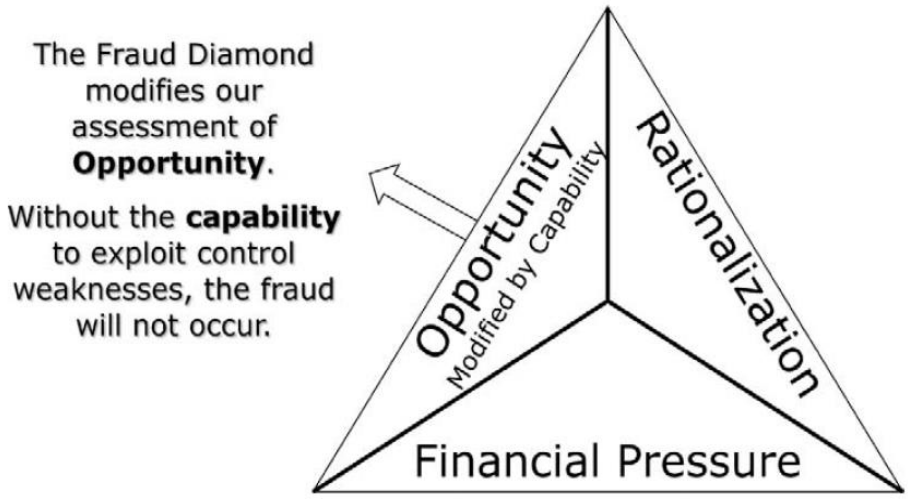

Figure 6. The impact of the fraud diamond on the fraud triangle (Dorminey et al., 2012)

2.2.6 The fraud predator

The predator theory removes the need for pressure and rationalization from the fraud triangle. There are two types of fraudsters, the first time or accidental fraudster and the predator. The first time or accidental fraudster is described by association of certified fraud examiners as being high educated, middle aged, trustworthy, usually has a position of high responsibility and is considered a respectable person by the public. The fraud triangle says that this person has only committed the crime because he was faced with a non-shareable financial problem, opportunity and rationalization but otherwise a good person (Association of certified fraud examiners, 2009). However according to Cressey the need for rationalization quickly disperses after committing the first fraud (1953). When this happens accidental fraudsters start to show the behavior of a predator. Not all authors agree that this happens some describe a group of accidental predators and people that are born as criminal (Dorminey, Fleming, Kranacher, & Riley, 2012). Predators replace the concepts of pressure and rationalization from the fraud triangle with respectively arrogance and a criminal mindset. Pressure and rationalization are no longer necessary to commit a fraud.

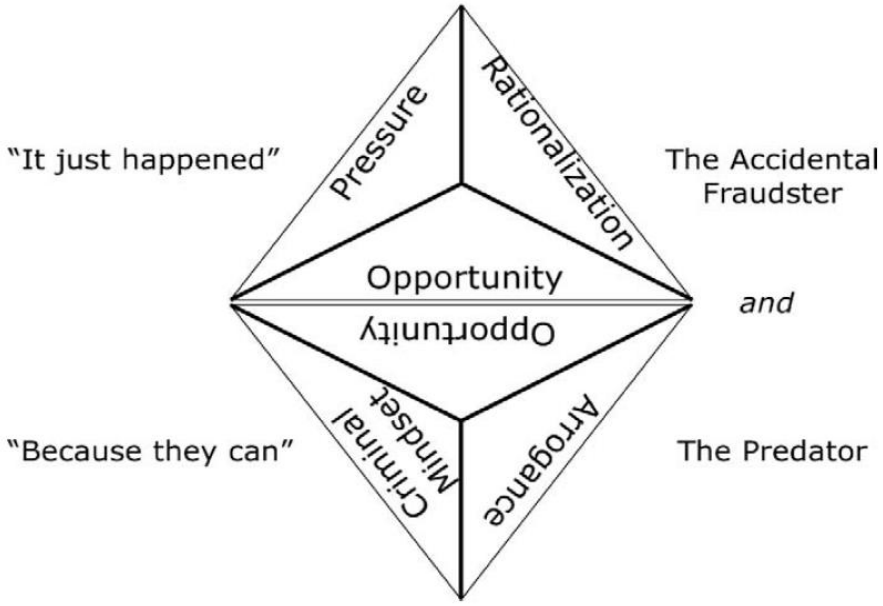

Figure 7. The accidental fraudster versus the predator. New fraud diamond emerges with a common element (Dorminey et al., 2012)

2.2.7 Weaknesses to internal control identified by the fraud triangle

Dorminey et al. (2012) derive the following reasons for the inefficiency of internal control from the fraud triangle: (1) budgetary constraint, (2) the costs of preventing every fraud exceeds the benefits, (3) people that constantly work with internal controls will learn their weaknesses, (4) management override and (5) collusion. Anti-fraud tools can be used to prevent, detect or deter. Tools that are to prevent the fraud are aimed at reducing the opportunity, the opposite side is deterrence that aims to create an environment in which fraud is unlikely to occur. The two strongest deterrents are fear of getting detected and fear of punishment. Detection tools are used to detect the fraud but are also a deterrent because they increase the chance of being detected if the employees are aware of the detection tools that is. Accounting internal controls are an example of a mechanism that aims to prevent fraud. The first reason why internal controls might prove to be ineffective is budgetary constraint. The cost of preventing every fraud exceeds the benefits and therefore choices are made. Second the changing business environment is always becoming more complex, this makes internal controls that were once effective ineffective. Third people that constantly work with the internal controls will learn their weaknesses and thus opportunity to commit fraud will eventually present itself. But even when internal controls that

segregate duties among several different people are in place (4) management override and (5) collusion might bypass the system (Dorminey, Fleming, Kranacher, & Riley, 2012). Usually the fraud triangle considers fraudsters to operate alone. But the most costly of financial statement frauds are collusion or management override according to the association of certified fraud examiners (2008). According to a report by AICPA when there is collusion internal controls are generally ineffective (2005). This is because internal controls are generally aimed at preventing one person from controlling every aspect of a transaction. In addition to this internal controls are aimed at separating custody, approval and accounting. Collusion works around internal controls to circumvent detection, while management override simply voids controls by self-reporting that no fraud took place (Dorminey, Fleming, Kranacher, & Riley, 2012).

2.3 Internal control

2.3.1 The definition of internal control

The committee of sponsoring organizations (COSO) defines internal control as follows:

"Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance (p. 3, 2013)."

This definition is very broad because the last fifteen years a shift has been taken from the focus on the accounting and finance view of internal control to the much broader governance and perspective view (Maijoor, 2000). Before the shift the term 'internal control' was interpreted as accounting controls, the system that auditors test as part of the assurance they provide on financial statements (Pfister, 2009). Pfister (2009) distinguishes two views: the focused view and the comprehensive view.

The focused view equals internal control to the checks and balances in accounting systems. A definition of the traditional or focused view of internal control is provided by Simons: "The detailed, procedural checks and balances" (1995, p. 84). These internal controls are designed to protect assets from misappropriation and to make sure that financial statements are accurate. Simons (1995) identifies three categories of checks and balances. (1) Structural safeguards which include an audit committee, an internal audit, segregation of duties, restricted access to assets and defined levels of authorization. (2) Staff safeguards that include expertise and training for all audit/accounting staff, rotation of jobs and sufficient resources. (3) System safeguards including

record keeping, documentation, audit trail, management reporting, and restricted access to information systems (Simons, 1995).

The comprehensive view emphasizes operational effectiveness, efficiency and dealing with laws, regulations and internal policies. An example of the comprehensive view is the framework provided by the commission of sponsoring organizations (COSO). COSO created the framework in order to provide broadly accepted criteria for establishing, monitoring, evaluating and reporting on internal control (COSO, 2013). Kinney (2000) states that COSO's framework is widely accepted in practice, as other organizations apply similar definitions. Examples of these organizations are: Canadian Guidance on Control Board (CoCo), The Institute of charted accountants in England and Wales (ICAEW), and the European federation of accountants.

2.3.2 The five key concepts of internal control

According to COSO Internal control has five key concepts. (1) It is aimed towards attaining objectives in three categories: compliance with law and regulations, reporting reliability and effectiveness of operations. (2) It is a process that consists of ongoing activities and tasks. (3) It is affected by employees, not only about rules and procedures but also the actions that people take affect internal control. (4) It provides ability for reasonable assurance to management, never absolute assurance in attaining objectives in three categories: operations, compliance, and reporting. (5) And last it's adaptable to the organizations structure (COSO, 2013).

COSO describes that internal control consists of the (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring (COSO, 2013).

The control environment is the set of standards, processes and structures that supplies the foundation for how the organization carries out internal control. The management team is responsible for setting up the tone at the top concerning internal control which includes the expected code of conduct. Managers strengthen these expectations across the company. The control environment contains the ethical values and integrity of the company, the limits that enable the board of directors to complete their governance oversight responsibilities, the companies structure that contains the assignment of authority and responsibility, the methods of attaining, developing and retaining employees, the strictness around performance measures, incentives, rewards, that are to drive accountability for performance (COSO, 2013).

All companies face different sorts of risks both from internal and external sources. Risk assessment is a process for recognizing and evaluating risks to the attainment of company goals. Risks are defined as the possibility that an event will occur that has an effect on the likelihood that a company attains its goals. Risks to the achievement of company goals are compared to risk tolerances that are established. Therefore risk assessment is the foundation for deciding how risks will be managed. Management should perform a risk assessment of the chance that the quality of the financial reporting process is affected by internal or external factors (COSO, 2013).

Control activities are the actions that are there to ensure that the actions established by the rules and procedures made by the management team to mitigate risks to the attainment of companies goals are carried out. Control activities can be both preventive and detective, and contain a range of manual/automated activities. Examples are: Authorizations and approvals, verifications, business performance reviews and reconciliations. Segregations of tasks is usually build in selection and development of internal control, when it's not practical then management considers other options. Control activities related to financial statements have the purpose to prevent, detect and correct errors in the financial statements (COSO, 2013).

Information is obtained by management in order to carry out internal control responsibilities so that companies' goals can be supported. The management obtains information that is both relevant and qualitative, from both internal and external sources in order to support the functioning of other components of internal control. Internal communication is the way information is shared throughout the company up and down. It helps employees to understand the importance of internal control (COSO, 2013).

Monitoring activities are a combination of ongoing evaluations and separate evaluations that measure if each of the five components of internal control and each principle within each component is present and functioning properly. Findings are evaluated against norms set by regulators, standard setting organizations, or the management team. Deficiencies are reported to the management team (COSO, 2013).

2.3.3 Internal control system

In the comprehensive view the internal control system is part of the whole system. Simons (1995) defines an internal control system as follows: "formal information-based routines and procedures that are used by managers to maintain or alter patterns in organizational activities. (p.

5).” In other words when speaking of the internal control system one means the formal mechanism of balances and checks. Internal control in contrast also encompasses informal control systems. An example is segregation of duties is part of the internal control system, whereas an informal discussion between two managers is part of internal control but not of the internal control system.

2.3.4 Hard- and soft controls

The "hard controls" can be defined as measurable agreements and guidelines. Often it is possible to measure these controls because they are rules set in an organization. Hard controls are thus based on rules and compliance. Measures that directly lead to visible different behavior or actions. Important in these measures is that they are easy to monitor and to test (De Heus & Stremmelaar, 2000). Hard controls are the more formal measures, such as an explicit code of conduct identified in a document (Vink & Kaptein, 2008). The hard measures are therefore mainly affected by "harder" aspects of the organization, such as planning and control, tasks, responsibilities and competences (De Heus & Stremmelaar, 2000). Hard controls aim to enforce desired behavior, for example by procedures, job separations and administrative systems (Kaptein & Wallage, 2010). Soft controls are all non-tangible but behavioral factors in organizations that can help to realize goals and manage risks. They do not come in place of rules, protocols or procedures. Such hard controls are also needed to clarify what behavior the organization desires. But hard controls prove ineffective if they are (in the absence of well-developed soft controls) misunderstood, circumvented or even used (KPMG, 2016).

2.3.5 Corporate governance

In the comprehensive view internal control is seen as an integrated concept in corporate governance (Pfister, 2009). The Organization for Economic Co-operation and Development (OECD) define corporate governance as follows (2004):

“A set of relationships between a company’s management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. (p. 11).”

This definition shows that in comparison to internal control corporate governance is more focused on the discrepancies between the goals of shareholders and top management. This discrepancy is also known as the principal-agent problem or the agency theory (Eisenhardt,

1989). The principal agent problem occurs when the agent is able to make decisions on behalf of the principal, but the agents might be more motivated to act in their own interest. An example of this is it's in the best interest of shareholders (principal) to receive accurate financial statements however top management (agents) might be motivated by bonuses to use creative accounting or financial statement fraud to make the financial position appear better than it actually is. Too that extend shareholders (principal) hire external auditors (agent) to make sure that financial statements are accurate. However it happens that shareholders delegate the tasks of appointing an external auditor to top management. In this situation the external auditor (agent) might be more motivated to keep top management satisfied, than to provide accurate information to the shareholders (principal) (Eisenhardt, 1989).

2.3.6 Essential components of internal control

In order to reduce the effects of problems like the agency principal problem organizations should have an effective internal control system. Rezaee & Riley (2011) define essential components of internal control as: (1) Tone at the top, (2) control environment reflected in structure, functions and risks, (3) control activities designed to achieve the control goals, (4) continuous monitoring, (5) communication of established activities, (6) proper implementation and enforcement of control policies and procedures. Pfister (2009) describes that internal control is effective when top management has reasonable assurance that: (1) they have information about if and too what extend operational effectiveness and efficiency are achieved. Operational effectiveness focusses on output- and operational efficiency focusses on input -of operations. Management needs to have a clear understanding of too what extend goals are attained (COSO, 2013). (2) Financial statements that are published and internal reports are accurate (COSO, 2013). The measurement methods need to be carefully applied and reporting should reflect the results correctly (Kinney, 2000). (3) The organization meets laws, regulations and internal rules that are applicable (Canadian Institute of Chartered Accountants, 1995). The organization complies when records meet the requirements such as production standards, accounting standards and tax requirements (Kinney, 2000). Merchant (1985) says internal control is effective when an informed person can be reasonably sure that no surprises will happen. Internal control provides confidence and effective internal control lowers the risk of fraud. It protects the organizations assets from theft and prevents distorted financial statements (Canadian Institute of Chartered Accountants, 1995). Effective internal control is also important to the organizations

environment. For example the financial statements are used by external decision makers, and is the main way of shareholders to have insight in the organizations earnings and financial conditions (Kinney, 2000).

2.3.7 Material weakness

Internal control is not effective when it has a material weakness. The Securities and Exchange Commission (2007) and Public Company Accounting Oversight Board (2007) define material weakness as a deficiency in internal control that leaves a reasonable possibility that a material ineffectiveness and inefficiency in operations, a misstatement in financial statements or nonconformity with internal or external rules and regulations will not be detected or prevented in time. The PCAOB (2007) define two types of internal control deficiencies: A deficiency in design and a deficiency in operation. A deficiency in design is when an internal control is missing or the design is poor so that even if the internal control would work as intended it would not achieve the objective. A deficiency in operations is when an internal control is well designed but does not operate as designed, or the person in control does not have the competence/authority to perform the control. Deficiencies in internal control are negatively correlated to internal control effectiveness (Pfister, 2009).

2.3.8 Limitations of internal control

While internal control can be effective it has its limitations, one of those is that internal control will only provide reasonable assurance instead of absolute assurance (Pfister, 2009). Pfister (2009) identifies two main limitations of internal control: (1) People that are in charge can make errors and omissions, or commit fraud. (2) The benefits may be perceived lower than the costs. COSO (1992) provides some examples of what can go wrong, even when internal control is well designed:

"Personnel may misunderstand instructions. They may make judgment mistakes. Or they may make errors due to carelessness, distraction or fatigue. An accounting department supervisor responsible for investigating exceptions might simply forget or fail to pursue the investigation far enough to be able to make appropriate corrections. Temporary personnel executing control duties for sick or vacationing employees might not perform correctly. System changes may be implemented before personnel have been trained to react appropriately to signs of incorrect functioning. (p. 80)."

In addition to these examples there is also the risk of management override for personal gain or to hide the company's true performance. Besides individuals two or more employees can circumvent internal controls by collusion. Internal control attempts to minimize all these risks but cannot provide a hundred percent guarantee of them not happening. When designing an internal control system management have to take into account the costs and benefits (Kinney, 2000). Figure 8 shows that the total cost is made up of decision error cost, asset loss, and residual risks and of the total amount spend on internal control. Past a certain point investing in internal control system is no longer efficient as there is always some residual risk (Kinney, 2000). The ability to invest in internal controls is constrained by time and resources available. A poor performing organization might not spend as much on internal controls because they focus on their core business and save on costs (Krishnan, 2005).

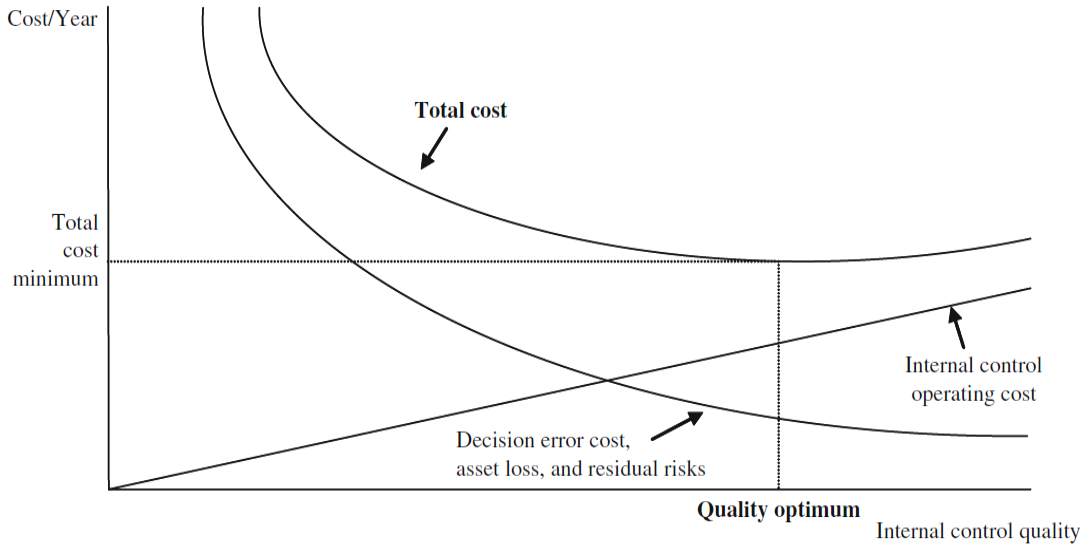

Figure 8. Cost and benefit of internal control (Kinney, 2000).

2.3.9 Relation between financial statement fraud, the fraud triangle and internal control

Figure nine shows the relation between financial statement fraud, the fraud triangle and internal control. Opportunity, rationalization and financial pressure increase the probability of financial statement fraud occurring. Once all three are sufficiently met the act of financial statement fraud occurs. Internal control is set in place to reduce the opportunity and to detect rationalization, and pressures. This lowers the probability of financial statement fraud occurring (Dorminey et al. 2012).

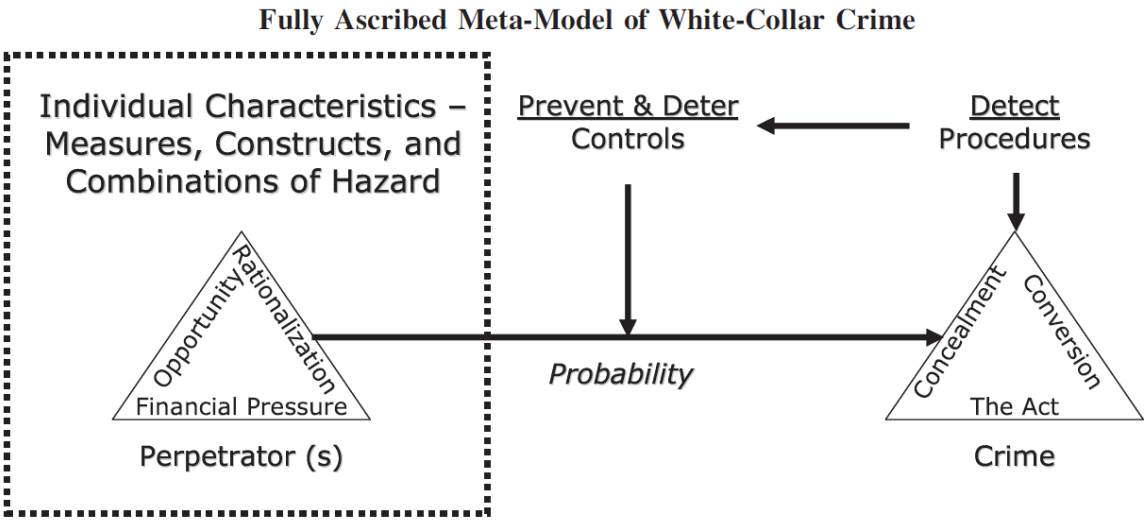

Figure 9. Fully ascribed meta-model of white collar crime (Dorminey et al., 2012).

3 Methods

In this chapter my choice for choosing a qualitative research method will be explained. The first step in doing this research was reading studies already done by other authors on the subject of financial statement fraud. By looking at their research methods, the pros and cons of different methods were identified. The first study that was read is a multiple case study done by Alexander Schuchter and Michael Levi (2015). In their study they interviewed respectable white collar offenders with high professional standing in order to show that perceived pressure is the main cause leading to fraud. In addition they show in their study that financial incentives are not required in order for someone to commit fraud. The second study is a systematic literature review done by Ahmad Kabir Usman and Mahmood Hussain Shah (2013). They choose a systematic literature review to provide the readers with critical success factors in preventing e banking fraud. Although a systematic literature review is good as introduction, it does not provide any new evidence regarding the topic of financial statement fraud. Therefore a systematic literature review is not used in this research. The third study that is reviewed is done by Benita Gullkvist and Annukka Jokipii (2013). In their research the authors examine whether auditors perceive the importance of red flags differently across two fraud types. To do so they collected over 400 responses using a web based survey. While this provides a lot of general information, the research question of this paper requires more in depth information and therefore a survey is not appropriate. The last research that is analyzed is written by Stolowy, Messner, Jeanjean and Baker (2013). The paper is a single case analysis of the Madoff fraud. However single case analysis provides a lot of in depth information it lacks any generalizability. Because in this research the aim is to provide insights on why internal controls failed to prevent fraud, a multiple case study is chosen as research method.

3.1.1 Qualitative research

In this chapter the methods used in this research will be discussed. Qualitative research is a method that in contrast to quantitative research has the goal of building theories instead of testing them. Other differences can be found in case selection. Quantitative methods often use random sampling to make sure their sample is representative of the population. However qualitative methods often use purposive selection in order to be able to get enough information to build a case. Summarized an advantage of qualitative research is that is allows for generating very

detailed and exact information about a small number of cases. However disadvantages are that it requires a lot of time and generalization to the population can only be done in a very limited way (Flick, 2011). In this research we are trying to explain why internal controls failed to prevent fraud in Dutch organizations and therefore qualitative research fits the design better.

3.1.2 Research process

In this study the research process for qualitative research as recommended by Flick (2011) will be followed. According to Flick qualitative research begins by selecting a research problem. In this research the problem is the financial damage that is caused by financial statement fraud each year. Second a review of existing literature will be done in order for the researcher to get a good understanding of the topic in question. Third the research question is formulated. In this thesis the research question is: 'Why internal control systems failed to prevent fraud in major Dutch organizations?" Fourth the research design is developed, because this is a qualitative research focus is on what cases to study, and who to interview? Fifth the interviewees and cases are selected. During the sixth step access to interviewees is secured. The seventh step is sampling of the cases. As this is a qualitative research the cases to be studied are selected according to their relevance on the topic of financial statement fraud. Once the cases and interviewees are selected the data is collected, documented and analyzed.

3.1.3 Research strategy

When choosing a research strategy three conditions are important: (1) the type of research question, (2) the extent of control an investigator has over actual behavioral events, and (3) the degree of focus on contemporary as opposed to historical events (Yin, 2003).

Strategy	**Form of research question**	**Requires control of behavioral events?**	**Focuses on contemporary events?**
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archival analysis	Who, what, where, how many, how much?	No	Yes/no
History	How, why?	No	No

Case Study	How, why?	No	Yes

Figure 10. Relevant research strategies in different situations (Yin, 2003).

The first condition covers the research question. In basis research questions provide answers on questions that begin with: ‘who’, ‘what’, ‘where’, ‘how’ and ‘why’. If research questions focus on what questions there are two options. The first option is when the research question is explorative, in that case any of the five strategies can be used. If the question is not explorative then a survey or archival analysis is more appropriate. In addition to these how many and how much questions also favor survey or archival analysis. These research strategies are at their best when the goal is to explain the prevalence of a variable or when trying to predict a variable. Contrast to these questions are how and why questions, researching why something happens requires more information which can be obtained by studying secondary sources and by conducting interviews. This research will provide an answer on a why question, therefore the first condition advises to use a multiple case study (Yin, 2003).

The second condition is extent of control over behavioral events and the third condition is degree of focus on contemporary events. History is the best strategy when there is no access or control, this is dealing with the past when there is no one to observe or interview and data must be obtained from sources like old papers or artefacts. The case study uses many of the same sources of information as history but it adds two. These are direct observation of the variables being studied and interviews with people that are involved in the research topic. The case study’s greatest advantage is the option use many different kinds of evidence like documents, artifacts, interviews and observations. Researchers do experiments when they need to manipulate behavior directly, precisely and systematically. Yin (2003) states that: “*The perfect situation for a case study is when a how or why question is being asked about a contemporary set of events, over which the investigator has little or no control (p. 9).”* This cite exactly describes the situation of this research, and therefore the multiple case study has been chosen.

A case study is a research strategy. Other options are experiments, surveys, histories and the analysis of archival information. Each research strategy has its own advantages and disadvantages. Depending on the situation each research has its own strategy, the best strategy for a research depends on: (a) the type of research question (b) the control an investigator has

over actual behavioral events, and (c) the focus on contemporary as opposed to historical phenomena. In general case studies are the best research design when "how" or "why" questions are being asked, when the researcher has little or no control over events, and when the focus of the research is on a contemporary phenomenon (Yin, 2003). According to Yin most researchers only repeat the types of topics on which case studies have been used when they give a definition. While other research especially in social sciences do not even recognize the case study as a research strategy. Yin (2003) the following definition of case studies in his book:

'A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident. The case study copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result. Last a case study benefits from the prior development of theoretical propositions to guide data collection and analysis (p. 13-14).

A different definition is provided by (Simons, 2009): *'A Case study is an in-depth exploration from multiple perspectives of the complexity and uniqueness of a particular project, policy, institution, programme or system in a 'real life' context. It is research-based, inclusive of different methods and is evidence-led. The primary purpose is to generate in-depth understanding of a specific topic (as in a thesis), programme, policy, institution or system to generate knowledge and/or inform policy development, professional practice and civil or community action (p. 21).*

Multiple case studies have different advantages and disadvantages when compared to single case studies. The evidence provided by multiple case studies is often found to be more reliable, as opposed to single case studies (Herriott & Firestone, 1983). However a downside of multiple case studies is that they require a lot more sources (Yin, 2003).

Yin (2003) advises researchers to do multiple case studies because even when doing a two case study the chances of doing a good case study will improve over doing a single case study. First this is because even with only two cases the research will be able to apply direct replication. Second the context from both studied cases will probably be different, if you can arrive at the same conclusions from multiple cases this will improve the generalizability of the research.

3.1.4 Sampling strategy

As multiple cases are needed they need to be sampled from a larger pool, this requires a sampling strategy. In this research theoretical sampling is used as sampling strategy. Theoretical sampling is developed by Glaser and Strauss (1967) who give the following definition:

"Theoretical sampling is the process of data collection for generating theory whereby the analyst jointly collects, codes and analysis his data and decides what data to collect next and where to find them, in order to develop his theory as it emerges. This process of data collection is controlled by the emerging theory (p. 45)."

In practice this means that cases are selected based on the amount of information they can provide in answering the research question. Interviewees are selected based on their experience with fraud prevention and detection, all the interviewees work at KPMG at either the forensic or the audit department. Case selection is based on the amount of available information, which means that the larger most well-known fraud cases in the Netherlands will be used for this research. This sampling strategy has been chosen because it allowed the research to focus on the cases that are most important to the research question. I selected ten well known fraud cases because of the large amount of secondary information that was publicly available. This way it was possible to get information about how and why the internal control systems that were present failed. Ten cases provided enough information to answer the research questions. In addition six interviews were held. The number of interviews was decided in consultation with KPMG, because of the seniority of the interviewees who together have audited hundreds of Dutch organizations six interviews provided enough information to answer the research questions.

3.1.5 Methods of data collection

Data needs to be collected on the sampled cases. Two methods have been chosen for usage in this research namely a qualitative analysis of documents and semi structured interviews.

Secondary data means data that was not collected for this research project (Flick, 2011). This data will be used to see why internal controls failed in major Dutch fraud cases. The advantage of analyzing secondary data is the data does not need to be collected thus saving time. The following problems arise from secondary data: (1) data needs to provide an answer the research question, (2) data needs to fit the research question, (3) the raw data is not available (Flick, 2011). The interview was chosen as second method because it is one of the most important sources of case study information (Yin, 2003). There are two ways of doing interviews structured

and unstructured. In structured interviews a predetermined list of questions is asked to the respondent. Advantages of this are that it can be administratered and coded easily. This form is close to a questionnaire. Unstructured interviews are like having a conversation, the idea is that interviewees decide the direction of the interview and the researcher listens (Flick, 2011). For this research a semi-structured interview was chosen. This combines the best of two worlds as it sets the structure with a list of problems to discuss, while allowing free space for going deeper on interesting topics. The structure is set by an interview schedule on which the topics to discuss are described (Thomas, 2011).

3.1.6 Methods of data analysis

Collected data will be analyzed using the CRIME model. The CRIME model was developed by Rezaee and Riley in 2011, and its primary goal is to order analysis of financial statement fraud. The five letters in CRIME stand for: (C)ooks, (R)ecipies, (I)ncentives, (M)onitoring and (E)nd results. The first letter from the word crime stands for cooks. Cooks provides an answer on who committed the crime, and what position was the fraudster in. The COSO report shows that about 80% of financial statement fraud is committed by CEO's or/and CFO's (1999). Almost all financial statement fraud happen with the participation/knowledge of top management (Rezaee & Riley, 2011). In this research the first letter will describe who committed the crime, and in what position the fraudster was. The second letter from the word crime stands for recipes. This describes the way the financial statement fraud was committed. Most financial fraud cases involve the manipulation of reported financial statements. Overstating of revenues by recording revenues too early or making fictitiously revenues is the most common recipe (Rezaee & Riley, 2011) (COSO, 1999). The second letter will describe the scheme of financial statement fraud and how it was committed. The third letter stands for incentives, which explains the reason why people or companies commit financial statement fraud. The most common reasons as identified by former research is: (1) goals and objectives, (2) covenants, (3) bonuses, (4) attracting new capital, (5) earnings per share and last (6) improve market perception (Rezaee & Riley, 2011). The third letter will try to describe the incentive for the financial statement fraud, however often times this is hard to say with 100% certainty even by experts in the field. The fourth letter stands for monitoring. The most important aspect of preventing and detecting financial statement fraud is corporate governance, the tone at the top should demand that financial statements are of high quality and misstatements should not be tolerated. Second to corporate governance in preventing

financial statement fraud is the focus of this research internal control. Internal control is the responsibility of the management team however other parties like external auditors should make sure an effective internal control system is in place and should make sure as much as possible management override is prevented as much as possible. The fourth letter will describe what internal controls were present and how they failed to prevent/detect the financial statement fraud which makes this the most important result of this research. The fifth letter stands for end results. End results describes what was gained / lost from the financial statement fraud. Examples are gain for the perpetrators or bankruptcy for the organization. Other examples are losing stock value, change of owners and delisting of the organizations. Some personal consequences for perpetrators are losing value of stock based compensation, being fired, being barred from even being in a management position again, being sanctioned to pay fines or to jail. In addition to these consequences for the company and the perpetrators other parties can also face adversarial consequences. Like when an external auditor suffers reputation damage from not having been able to detect the fraud, while this is practically impossible and only happens in 10% of the fraud cases. An estimation of the costs of the recent mortgage crisis which was caused by corporate irregularities are around 1.5 trillion US dollars. In this research the fifth letter will describe the financial consequences for the organization, examples are resources stolen, fines or in case of liquidation shareholder value lost. In addition to the case analysis the interviews will be analyzed. The interviews aim to answer research question two and three. Different interview questions have been created. Each question can be divided in two groups each helping to answer one question. The answers to all questions were lined up on a per question basis and similarities were found and reported in a summarized tables.

3.1.7 Conclusion

This research uses a multiple case study as its research method. This research method was chosen because this thesis will provide an answer on a why question. In addition to this the research does not require control of behavior from the cases. Last the research focusses on contemporary events. The thesis will look at multiple cases mainly to improve generalizability. Data will be collected from a sample selected by theoretical sampling, which means those cases are selected that provide enough information on the topic. The data will be collected by doing a secondary research on major fraud cases in the Netherlands and by interviewing auditors and forensics working at KPMG.

4 Results

4.1 Financial statement fraud case analysis

In this section ten reported financial statement fraud cases are analyzed in light of the five fraud factors: Cooks, Recipes, Incentives, Monitoring and End-Results (CRIME) (Rezaee, 2005). The results of the case study help to answer the first question: "How was financial statement fraud commited at major Dutch organizations?" Table 1 summarizes the results in paragraph 4.3.

The foundation of Royal Imtech started to crumble, when the big German part of the technical services of Gouda filed for bankruptcy. The company just celebrated its 150-year anniversary in 2010, but three years after this anniversary they received a substantial blow after years of fraudulent activities in Germany and Poland came to light in 2013. Since then Imtech tries to scramble back up, so far with little success. The Company reported a loss of more than half a billion euros on a total sales of 3.9 billion euros. It went wrong for Imtech in the construction of an amusement park in Poland. In July 2012 Imtech made the order, the largest project in the history of the company, from 620 million euros public. But the mega project never became reality. Imtech eventually had to write of € 370 million in Poland. A reconstruction of Het Financiele Dagblad (FD) showed that Imtech in 2011 and 2012, with the knowledge of the board, through complex financial structures financed their own investment. Although there were no financiers or permits, former CEO René van der Bruggen approved the project. Also family members of Imtech's board members owned shares in companies that were behind the theme park, creating a conflict of interests. Ultimately through the failed project the fraud in Germany and Poland was revealed, which saddled the company with more problems. The former CEO of Imtech Germany paid an unknown party who Imtech Netherlands calls the "Group X" approximately $ 30 million for which no legitimate business justification was found. In his defense director of the German branch Klaus Betz states that ten years of accounting tricks, sham accounts and illegal transactions on behalf of the then chief executive of the parent company René van der Bruggen, Imtech Netherlands boosted the figures. That Betz said in testimony he gave behind closed doors in October 2014 with the Public Prosecutor in Hamburg. The fraud forced the company to collect € 500 million in a rights issue to replenish the finances. The ICT branch of the company was sold for € 255 million euros. The interventions were needed to alleviate the debt burden of more than 1 billion euros. How could it come to this? Royal Imtech

was in 2012, grown into a mega group, which with 23,000 employees working in more than 27,000 different projects in almost all European countries. Many more projects than can naturally be overseen by a board of directors. The then board of Imtech in Gouda, led by René van der Bruggen, laid the responsibility for the successful completion of these projects with approximately one hundred managers, whose variable remuneration was unilaterally pegged to the growth in sales and operating profit. History - from Ogem and RSV, the American energy giant Enron and Ahold supermarket group - shows that such a decentralized governance model should be accompanied by strict control, clear reporting lines and an open, transparent corporate culture. Otherwise it is guaranteed to go wrong. Because aspiring managers start being creative with the numbers to achieve their ambitious goals (Nods, 2015). The cooks of this financial statement fraud were the director of the German branch, and middle management who overstated revenues. The director hid his fraud by withholding the books from the headquarters. Middle management hid the overstatement of revenues by reporting non-cash items as cash. The most important incentive was the excessive bonus culture. Monitoring this fraud scheme was hard because the organization was growing so fast, internal control could not keep up. Normally internal audit departments would warn for this, but Imtech did not have one. An internal control that compared cash flows to revenues could have detected this fraud earlier but was absent. Fraud came to light thanks to research by KPMG and a whistleblower. The result of this fraud case was that Imtech had to file for bankruptcy, over 2.5 billion shareholder value was lost. Half of this damage was taken by banks, half by shareholders. The director of the German branch was convicted to four years in prison.

In February 2003, the problems for Ahold became Visible. Reported sales of Ahold's subsidiary Foodservice were more than 800 million dollar too high in the financial statements. This was because US Subsidiary Foodservice reported purchase bonuses however did not make the right quantities. If the quantities were not realized the bonus was not received, or on a reduced scale. The practice at the Amerika2Use subsidiary, however, was that they reported bonuses they would not receive in practice. In addition to this fraud Ahold also pretended to have full control over its subsidiaries which was not the case because of this sales were reported too high for years. To consolidate you need to have a majority of control. Ahold published so called control letters claiming they were in control of the subsidiary. However Ahold also wrote side

letters in which they denied to have control over the subsidiaries. These letters have been kept secret to Ahold's Board of Statutory Auditors and the house auditor Deloitte. The criminal proceedings in the Netherlands focuses on issues consolidation of joint ventures, control letters and side letters (Kasteleyn & Vrijbloed, 2006). The cooks of this financial statement fraud are Ahold's then top management. Subordinates overstated revenues by counting purchasing bonuses which were not met. Ahold Overstated revenues by withholding information from the external accountant. Ahold consolidated statements of subordinates in which they did not have a majority interest. This is not allowed and is how Ahold could make their revenues seem higher for years. Incentives for this fraud were growth goals of 15% per year, when the average growth rate in the branch was 1%. Large bonuses were tied to these high goals which caused management to commit fraud in order to achieve the goals. The consolidation fraud is hard to detect because management created two contracts. The contract that was shown to the external auditor, said that Ahold had a majority interests and therefore consolidation was allowed. However the real contract was withheld from external accountants. The fraud from Ahold's subordinates could have been detected earlier if Ahold had a centralized cash and treasury management in place by taking feeds from ERP systems and interfacing to external bank accounts, a centralized cash and treasury management system can deliver complete visibility of true cash flows in real-time, enabling discrepancies to be immediately identified. However such a system was not in place. The fraud eventually came to light by the new CEO, who started asking questions about the legitimacy of the notes. The fraud resulted in stocks going down with 63% leading to Ahold paying back investors a total of 1.1 billion USD.

The Dutch court sentenced a fraudster to five years in prison. Jeroen J. worked for the insurance company Delta Lloyd between 2005 and 2008. By committing forgery, he caused the company more than 4 million euros damages. According to the Dutch prosecutor contracts were falsified and fictitious invoices submitted. Delta Lloyd paid these bills. Through payments to limited companies the money flowed back to J., according to the Dutch prosecutor. In total there were six fake contracts and 61 fictitious invoices. The main suspect would not only have acted unconscionably and created an administrative apparent reality, he would also drag several contractors and even his family members with him. That the internal control of Delta Lloyd was very weak at some points, was no excuse for his fraudulent actions according to the Judge

(Algemeen Nederlands Persbureau, 2017). The cook in this fraud is Jeroen J. (middle management). He committed the fraud using false invoices. Motivation for the fraud was self-enrichment. According to the judge the internal control system was weak, giving Jeroen J opportunity. However it is not explained why the internal control system was weak. The fraud resulted in 4 million euro in damages to Delta Lloyd, and five years in prison for the fraudster.

The listed billion company SBM Offshore knowingly concealed facts about the nature and extent of corruption within the company for 2012 to 2015. According a whistleblower the board of the company was aware of the corruption since the beginning of 2012. The whistleblower also said that fraud is in the DNA of the company. SBM director Sietze Hepkema said in 2012: “I'm not here to nail people to the cross I'm not here to judge what is morally right or wrong, we have to run a business, I'm not going to turn over every stone... to identify any missteps in the past. ". In 2012, the whistleblower became involved in an internal investigation into corrupt practices, after documents about the corruption had surfaced within the company. Tens of millions of bribes were paid to win contracts in various countries around the world. In 2014, SBM struck a settlement with the Dutch public prosecutor for a record $ 240 million (192 million euros), the highest in Dutch history. In addition to a fine of 40 million, $ 200 million in wrongfully obtained profits were paid. With this settlement SBM prevented prosecution for corrupt practices in the Netherlands and the United States. However more cases are pending (Nederlandse omroep stichting, 2015). Cooks in this case are top management who willingly bribed government officials in order to obtain more orders. Internal control failed because corruption is accepted as part of the culture of the company. The fraud resulted in a settlement for $ 240 million, with more to come.

Three employees of Heineken were arrested in July 2007. Earlier that year they were involved in a massive fraud at the beer company. The trio, hired through an intermediary, managed to steal 2.5 million euro from Heineken. The three suspects wrote false invoices. The invoices were paid to firms that were owned by six other suspects. The Fraud went as follows: the money was first transferred to the bank account of Alexander BV (formerly Imexko BV) Rosmalen. Director was 59-year-old Marinus S., who was convicted several times in the past for fraud. S. booked the money to about 30 other persons or entities, including Vitatem BV. Alexander S. BV has been declared bankrupt, so there is nothing to lay claim to for Heineken. But Heineken cannot claim back their money from the other organizations either because they were according to realistic agreements. For example one organization received 100,000 euros from Alexander BV for the supply of a used Rolls-Royce Silver Seraph. And got yet another trader received 48,000 euros for jewelry and clocks. Fraud is difficult to prove in these transactions, and because Heineken cannot prove the organizations were in on the fraud, they cannot claim back their money (Libbenga, 2016). Cooks in this fraud case were three middle managers and their co fraudsters. The recipe that was used for the fraud was false invoices. The incentives were self-enrichment. The employees had authorization to select suppliers, order services and products, and authorize the payment, circumventing internal control systems through collusion. The result of the fraud was that Heineken lost 2.5 million euros.

Gross malpractices of three key figures within Innoconcepts led to the bankruptcy of the listed company. Auditor Deloitte was not able to prevent such practices and for years even approved the financial statements. Deloitte as accountant of Innoconcepts failed to notice that Innoconcepts had built up debts running in to the millions at around ten Chinese companies, these debts were not reported in the financial statements. According to the curator, the most basic rules of corporate governance were systematically ignored. The management structure at Innoconcepts is also described as "incestuous". And there was a conflict of interest between Innoconcepts on one hand and the private companies of board members Langerak, Teerlink and Highland on the other. Also president-commissaris Jansen Venneboer was no independent regulator. For example, he sent additional invoices for counseling in 2008 and 2009 for 50 thousand euro each in addition to his usual supervisory fee. Adequate supervision did not exist. According to the curator the financial resources of the company were squandered on a large-

scale. Only through recurring issues of shares (approximately 150 million shares were issued from 2004) liquidity problems could be solved temporarily (Vereniging van effectenbezitters, 2015). The cooks in this fraud case are the top management. They committed fraud by withholding information from their accountant. They committed the fraud in order to hide that the company was in financial distress. The internal control system failed because of failing corporate governance. The fraud resulted in the bankruptcy of Innoconcepts, over 380 million euros of shareholder value was lost. The company's board, Deloitte and ING were all sued by the curator. Deloitte settled for 18 million euros.

The director of the real estate branch and eight other ex-bankers enriched each other without knowledge of SNS. According to the Dutch justice department the case turns around two people: former board member Brucht "Buck G., who was arrested in February 2013 and spent six weeks in custody, and his right hand Pieter G. The two have received 2.3 million euros in bribes from the other suspects and through them they laundered false invoices. In return the suspects were offered jobs in the Property Finance department. False invoices had to conceal the bribes. Former director of the former real estate branch of SNS Reaal Buck Groenhof was sentenced by the Dutch justice department to a prison sentence of 1.5 years of which six months were suspended. The second main suspect got fifteen months, five of probation. The men were convicted of participating in a criminal organization, bribery, money laundering and forgery.

Buck Groenhof hired managers to address the financial problems in the real estate branch. With the help of the managers businesses they paid the two main suspects at least two million without awareness of SNS. Wage increases awarded to managers by Groenhof, flowed through to him. Even his secretary paid a portion of her salary to Groenhof under the guise of "advice and coaching." The prosecution found a total of three hundred false invoices. The court granted claims up to 2 million, in addition to fines of between 5,000 and 50,000 euros to their businesses. In February 2013, SNS Reaal filed charges to Groenhof, having examined mailboxes of him and other employees. The talks between the bank and investigation service FIOD were already underway. The FIOD did three years of research and found fifteen managers from SNS Reaal that enriched each other. Some of them settled, nine appeared before the court. The fraud has forced the state to nationalize SNS Reaal. In the case of SNS Reaal nationalization was inevitable. Quarter after quarter the banking and insurance division performed reasonable, but

the Property Finance department did terrible which lead to the group's losses. The Fraud in which the OM suspect fifteen managers has played a major role, although it is not clear whether that was a decisive role (Giebels, 2015). The cooks in this case are the director, his co offender and the middle management. They used false invoices to hide their fraud. The sole incentive for this fraud was self-enrichment. The internal control system failed because many employees both higher and middle management were co offending. The fraud was partly responsible for the nationalization of SNS Reaal, however the real estate branch was suffering losses even before the fraud. The nationalization of SNS Reaal cost the Dutch government 3.7 billion euros. The Dutch justice department filed charges against the fraudsters.

LCI was an IT company specialized in distributing desktops and printers. During the internet hype the company's stocks were on the rise. The ever rising share price was used by Chairman Asser as change for acquisitions, as the acquisitions were partly funded by shares. The shares are only paid when the companies perform well. This earn out method was a motivation for the acquired companies to perform well, and report every penny as turnover. Between 1993 and 2000 the turnover is multiplied by ten. The profit growth rate is more than forty percent each year. In 1997 LCI sues Motorola for 237 million euros and reports to shareholders that they expect a quick payout, while hiding that the claim has already been sold to a bank for 9 million euros. In 1998 a fraud is detected at CCW one of LCI's daughter companies. Thirty million euros disappears through artificially raised revenues, hidden by false invoices. When this came to light the stocks dropped by 56% on one day. Within the next two months LCI is forced to file for bankruptcy. A total of 300 million euros market value was lost (Vereniging van effectenbezitters, 2009). This fraud case actually consists of two frauds: The first fraud is committed by the LCI top management, when they hid the fact that they had sold the 237 million euro claim for 9 million from shareholders. The second fraud is committed by LCI's subsidiary, where the revenues were reported 30 million euros too high. Top management simply withheld the information from shareholders, claiming they are counting on 237 million. Middle management committed the fraud by way of false invoices. Both frauds were committed in order to meet high expectations from top management, shareholders and the outside market. An investigation reveals the following internal control related problems: (1) The one man management structure and absence of CFO led to an undesirable power structure at LCI. (2) The supervision of the

commissioners had failed. (3) A claim for 237 was knowingly wrongly activated. (4) The absence of a central organization made controlling LCI difficult (Vereniging van effectenbezitters, 2015). The fraud resulted into the bankruptcy of LCI, over 300 million euros shareholder value was lost.

Cash manager Marcel de Vries working for Vestia was responsible for controlling the derivatives wallet. In 8 years he almost earned ten million euros. He did this by buying derivatives from banks through intermediary Arjan Greeven. Greeven was paid provision with every deal, and transferred half of the provision to an account with the name Inventus, this account was owned by De Vries. The fraud came to light when Greeven confessed to the crime under pressure of guilt of his share in the financial distress Vestia was in. The informer gave his administration to Vestia and the Dutch prosecutor and explained his methods as well as the banks. Too hide the fraud de Vries tried had bank statements altered in such a way that they did not show Vestia they were paying provisions to Greeven. In addition multiple people were bribed, too hide the bribes false invoices were created (Gualthérie van Weezel, 2016). The cook in this fraud case is Marcel de Vries. He committed fraud by buying derivatives through an intermediary, taking half of the intermediary provisions. Too hide the fraud he altered bank statements to hide payments to the intermediary, and bribed other people. Bribes were hidden using false invoices. Self-enrichment is the sole purpose in this fraud case. The internal control system failed because Marcel de Vries colluded with Arjan Greeven, and bribed people that were supposed to check on him. The result of this fraud were disastrous for Vestia, only paying off the derivate costs more than 2.7 billion euros. This almost caused the biggest housing corporations in the Netherlands to be liquidized. The Dutch prosecutor filed charges against Marcel de Vries and Arjan Greeven. However the Deutsche bank was not sued for their part in the fraud.

KPN and the American Qwest merged their European optical fiber activities in 1998 in the joint venture: KPNQwest. The company was responsible for building 25000 kilometers of fiber-optic network in 18 countries. Then suddenly the company was unable to pay its bills and was forced to file for bankruptcy in 2002, leaving behind 4.2 billion euros of unpaid debts. Before that the company only fenced growing revenues and healthy profit margins. According to KPNQwest the bankruptcy was due to sudden drop in market prices. However research showed

that even in the founding year the market price already plunged by 40 to 80 percent due to overcapacity and increased competition. To the shareholders KPNQwest held the share decline in turnover hidden and they gave the impression that it had sufficient income to continue to achieve its objectives as laid down at the start. The company sold capacity on the fiber network to KPN, Qwest and others but these transactions were fake: the customers did not need capacity and paid for it with their own capacity, or the transactions said something was sold when in truth it was rented. The actual KPNQwest revenue for 2000 and 2001 was only half of what was reported. According to the trustees the reason for this fraud was not self-enrichment but holding out longer than the competition and thus gaining market share (Olsthoorn, 2010). In this fraud case the cooks are the top management, who willingly and knowingly colluded with other players in the market to create artificial revenue. They did so by renting out their fiber cable usage to KPN, Qwest and third parties. Ownership of fiber cable is often up to debate, so both parties booked the rent as revenue. Side letters like in the Ahold case were used to hide this fraud. Incentives were share price manipulation and self-enrichment of the Qwest board, who had shares in KPNQwest. Monitoring did bring the fraud to light internally, however resistance to these practices failed to change anything. Even externally a warning came in 2001, however the board of Qwest talked their way out of it. I did not help that Anderson was the external accountant, Andersen was one of the major five accounting firms but had to file for bankruptcy due to the many fraud cases plaguing the company. The fraud resulted in over 4.2 billion euros to be lost in debts, in addition to shareholder value.

4.2 Interview analysis

In this section the results from six interviews held with top management of one of the four major accountancy firms are described. The results from the interviews help to answer the second research question: “How do Dutch organizations create effective internal control systems?” and the third research question: “What dangers are there to internal control systems in Dutch organizations?”

Four out of six interviewees mention soft controls as well as hard controls when asked for fraud prevention best practices. Interviewee C (appendix 7.3.3) said the following about culture: *“The examples I just named are hard controls, but soft controls are just as important. Examples*

are tone at the top, or what kind of example top management sets. It is about the combination between hard and soft controls, one will not do the job."

An example of such a soft control is given by interviewee A who thinks it is very important that everyone carries responsibility for the financial statements. A sales department could detect artificially raised revenues by asking themselves did we really generate this much revenue? Or a purchasing department might realize that they had not purchased enough materials to generate this revenue. If the finance department has sole responsibility for the financial statement risk of fraud increases. Risk analysis is also named as best practice in fraud prevention. According to interviewee B it is impossible to create a good internal control system, without knowing what risks your organization faces. Another soft control that is brought up in the interviews is supervision, by a supervisory board and by an external accountant. Last two interviewees mention bonus policy, when the bonus part of an employee's payment is too large of a portion risk of fraud is increased.

All the interviewees mentions segregation of duties as most important hard control. According to interviewee C (appendix 7.3.3) this is because: *"It is easier to detect fraud when multiple people are involved in a process, for example who places a purchase order, who receives the goods or service? Who authorizes the invoice? If all these things are with one man or group, fraud becomes hard to detect."*

It is also important that controls are visible, visible means that third parties can see that the controls have been carried out. Other important controls are the four eyes principle, and a good mix between preventive and detective controls. This means that organizations should also have controls in the beginning of the process, and not only detective at the end. Another important control is authorization limit. Last proper budgeting towards your shareholders is important, because it does not allow for unrealistic expectations.

Internal control and efficiency is something that can bite. Small organizations wonder what the minimum investment to comply with rules and regulations is. Larger organizations are pragmatic, it should not cost too much. According to interviewee B (appendix 7.3.2.) this is a bad mindset: *"You should create a good internal control system in which you cover the right risks with the right controls to create an optimal mix and efficient internal control system."*

To do this organizations first need to map all their risks, by asking how to get money out of this organization? Then decide what their risk appetite is, risk appetite is how much risk the

organization wants to take. Less risk comes with higher risk premium, which is the cost for implementing controls on risks. After deciding the risk appetite organizations can identify the most critical risks, and put internal controls on those processes in order to create an efficient internal control system.

In the Netherlands IT is coming up as a fraud prevention method. An example of this is access management, which explains who has access to what part of an organizations financial systems. Interviewee A (appendix 7.3.1.) mentions that products are being made that are able to analyze data from ERP systems to find breaches in the internal control system. Other developments in fraud prevention methods are period reporting, monitoring and budgeting. An example of how this can go wrong is given by interviewee B (appendix 7.3.2.): *"Pressure from shareholders who expected unrealistically high revenues set by budgeting created an optimized setting for fraud."* Expertise at the top is another strategy, for example in a major Dutch fraud case it came to light that almost no one had sufficient knowledge of financial instruments.

According to interviewee A (appendix 7.3.1.) detection of fraud lies in strange things. Therefore accountants check trends and numbers for remarkable cases. Also data analysis is a new development. An example of something out of the ordinary that can be brought up by data analysis is when a CFO does a booking out of office hours. In addition to this organization specific risks like tradable or a bonus culture can be indicators that require further investigation. Last knowledge of the organization is named as being important to detect fraud.

One of the interview questions aimed to provide insight into the strengths and weaknesses of internal control. However interviewees explained that it is not so much about strengths and weaknesses, but that internal control is vital to the survival of an organization. Interviewee A (appendix 7.3.1.) said: *"Internal control is not so much about strengths/weaknesses but it is mandatory, an organization cannot exist without internal control."* Advantages are prevention and earlier detection of problems. Weaknesses are bad soft controls, breach of segregation of duties and excessive bonus systems.

Management override is considered by all interviewees as a serious threat to internal control systems. Interviewee C said: *"In all audits we see the risk of management override as a presumed risk, which means we assume that it is always present. In 9 out of 10 cases there can be motivation from management to direct results."*

In practice there are a few things organizations can do to make management override less likely. The most important being culture. It should be clear to all employees that fraud is not accepted. In addition to that there should be a whistleblower program, and it should be very clear within the organization where to report possible frauds. Last employees should attain a professional critical attitude towards management requests.

Collusion is considered a lot more difficult to detect by the interviewees, however they also consider it less likely than management override. The problem with collusion is that it requires a high level of trust between employees. The risk of collusion increases when employees find themselves in the same place for longer, this way they can bond with each other and with suppliers / customers. Collusion has a critical effect on internal control systems rendering them ineffective. Interviewee E (appendix 7.3.5.) said the following about collusion: *"The effect would be that the internal control system would fail. Internal control measures would cease to be effective."* The risk of collusion can be minimalized by making sure no employee stays on the same job for too long. In addition to that culture is named to be effective, it is more difficult to find people to collide with in an organization that does not have a culture to support fraud.

The effect familiarization has on internal controls is deemed small by the interviewees. They provide two main reasons for this. The first one is when weakness in internal control is revealed through familiarization with those controls, then the controls are not good enough or not carried out properly. The second holds true to larger organizations, where it is uncommon for employees to be on doing the same job for longer periods of time. Last internal controls system are not stable, what was proper internal control five years ago might not be sufficient any longer. Interviewee C (appendix 7.3.3.) said the following about familiarization: *"A lot of lower level for example administrative functions are filled by the same person for many years, however this does not mean that the risk of fraud becomes higher assuming the internal control system is strong enough."* Much like collusion interviewees advise to switch employees between processes, too prevent them from doing the same job for too long.

The interviewees agree that organizations have to make choices when investing in internal control. Investing too much or too little in internal control leads to inefficient systems. Interviewee D (appendix 7.3.6) said the following about internal control: *"Insight in the risks the organizations faces is very important. Then an organization has to decide its risk appetite, which*

is how much risk is it prepared to take. And those two together decide how much an organization has to invest in internal control."

Most interviewees think financial distress increases the risk of financial statement fraud. Interviewee G agrees however states that organizations that are in financial distress do not necessarily have less resources to spend on internal control. Instead the risk of fraud increases because things like bank covenants and shareholder pressure provide incentives. Interviewee A (appendix 7.3.1.) advises organizations to focus on soft controls: *"If the soft controls are working properly hard controls are in theory not really needed. Of course in practice you need the combination. Save on hard controls where possible, less period reports but keep investing in soft controls."* Other recommendations are automation of as many controls as possible and having a supervisory board.

When the interviewees were asked if any dangers to internal control systems had not been brought up yet many mentioned weak soft controls as a danger to hard controls. Interviewee C (appendix 7.3.3.) explains: *"When the culture is not right, internal control becomes less efficient. You should have enough attention for both hard and soft controls. Otherwise people set their signature where they have to, and for the rest adhere themselves to nothing."* Some people even go so far as saying soft controls are more important than hard controls, and that when an organization has proper soft controls in place hard controls are not needed. Of course in practice it is always about having a good mix of both. A different danger to internal control that was named is over expenditure, when internal control becomes unworkable employees are provided with an incentive to find workarounds. Another danger that was brought up is the gap of knowledge between management and shareholders. Last when doing business internationally there are different norms and values that might pose a risk to internal control systems. For example Chinese companies refused to share financial statements with the accountant in a major Dutch fraud case on the grounds of it being abnormal in China.

4.3 Summary of the results using tables and figures

Table 1 shows a summary of the cooks, recipes, incentives, monitoring, and end results of each of the cases described above.

Organization	Cooks	Recipes	Incentives	Monitoring	End Results
Imtech	Top and middle management	Fraud in Poland and Germany. Overstating revenues. Booking noncash items as cash. Unauthorized payments to relations without business purpose by with keeping booking systems from head office.	Excessive bonus culture	The Organization was growing so fast, internal control could not keep up. Normally internal audit departments would warn for this, but imtech did not have one. An internal control that compared cash flows to revenues could have detected this fraud earlier but was absent. Fraud came to light thanks to research by KPMG and a whistleblower	Over 1 billion in losses leading to bankruptcy for the organization. Organization is split up and sold. Before the first fraud the total stock value of imtech was 2.5 billion, previously to the bankruptcy stocks were worth less than a penny. About half of this loss is taken by banks, the rest by investors
Delta Lloyd	Middle management	Manager created false invoices and send them to 9 independent contractors. The contracters accepted the invoice and received the payment, of which the fraudster gained a share. In addition the private contractors worked on the fraudsters private projects.	Self-enrichment	The manager in question was responsible for the entire operation. Proper segregation of duties could have prevented this fraud. The fraud was detected when an employee of Delta Lloyd found out one of the invoices was invalid.	4.5 million euros. Most of it was paid back by the private contractors. Some by the fraudster.

Organization	Cooks	Recipes	Incentives	Monitoring	End Results
SBM Offshore	Top management	The organization bribed state officials to get orders. The payments were not reported to shareholders, on advice of the boards lawyers	Acquiring more orders	According to the whistleblower fraud is in the organizations DNA. As mentioned in this research a culture that allows fraud, renders any internal control systems useless. The fraud came to light when an internal research was done after documents about the fraud raised questions. After this research was kept quiet the whistleblower blew the whistle.	SBM Offshore settled with the justice department for 240 million USD, another settlement is in the making. Estimations are over 1 billion.
Heineken	Middle management	Three managers payed false invoices to the bank account of Alexander BV, from here the money was immediately transferred to 30 other bank accounts. However Heineken can't get any money back because the other bank accounts were payed reasonably. For example one hundred thousand for a rolls Royce. It is impossible for Heineken to prove that the owners of those organizations were in on the plot.	Self-enrichment	The internal control system detected the fraud, however the money was already gone. In this case three employees worked together to circumvent internal control, rendering controls that would otherwise be useful like segregation of duties or authorization pointless.	Total damages for Heineken are around 2.5 million euros. However some is retrieved through settlements with fraudsters.

Organization	Cooks	Recipes	Incentives	Monitoring	End Results
Vestia	Top management	Cash manager Marcel de Vries working for Vestia was responsible for controlling the derivatives wallet. In 8 years he almost earned ten million euros. He did this by buying derivatives from banks through intermediary Arjan Greeven. Greeven was payed provision with every deal, and transferred half of the provision to an account with the name Inventus, this account was owned by De Vries.	Self-enrichment	The fraud came to light when Greeven confessed to the crime under pressure of guilt of his share in the financial distress Vestia was in. The informer gave his administration to Vestia and the Dutch prosecutor and explained his methods as well as the banks. Too hide the fraud de Vries tried had bank statements altered in such a way that they did not show Vestia they were paying provisions to Greeven. In addition multiple people were bribed, too hide the bribes false invoices were created.	Vestia lost almost 10 million euros to the fraud.

LCI Computer	Top and middle management	In 1997 LCI sues Motorola for 237 million euros and reports to shareholders that they expect a quick payout, while hiding that the claim has already been sold to a bank for 9 million euros. In 1998 a fraud is detected at CCW one of LCI's daughter companies. Thirty million euros disappears through artificially raised revenues, hidden by false invoices. When this came to light the	Hiding performance, meeting ambitious goals.	An investigation reveals the following internal control related problems: (1) The one man management structure and absence of CFO led to an undesirable power structure at LCI. (2) The supervision of the commissioners had failed. (3) A claim for 237 was knowingly wrongly activated. (4) The absence of a central organization made controlling LCI difficult.	When this fraud came to light the stocks dropped by 56% on one day. Within the next two months LCI is forced to file for bankruptcy. A total of 300 million euros market value was lost.

Organization	**Cooks**	**Recipes**	**Incentives**	**Monitoring**	**End Results**
SNS Reaal	Top and middle management	Managers payed the director of the Property Finance department money to hire them. In turn the director granted the managers salary increases. This effectively created a money wheel. The fraud was hidden by over 500 false invoices.	Self-enrichment	After four complaints about the integrity of the director a research was started by The Nederlandsche Bank, the recommendation was to fire the director. However instead SNS Reaal appointed him as advisor, to circumvent the rules. Later the fraud was discovered when SNS Reaal searched the email boxes and reported the fraud to the FIOS. In this fraud case over 15 fraudsters worked together, circumventing and overriding internal controls.	Due to the financial performance of SNSPF, SNSReaal had to file for bankruptcy. This is to a large amount due to the fraud, but also do the financial crisis. In the end the Dutch government payed 3,7 billion to nationalize the bank.

KPNQwest	Top management	The company sold capacity on the fiber network to KPN, Qwest and others but these transactions were fake: the customers did not need capacity and paid for it with their own capacity, or the transactions said something was sold when in truth it was rented. The actual KPNQwest revenue for 2000 and 2001 was only half of what was reported.	According to the trustees the reason for this fraud was not self-enrichment but holding out longer than the competition and thus gaining market share.	Fraud came to light because of bankruptcy. Then suddenly the company was unable to pay its bills and was forced to file for bankruptcy in 2002, leaving behind 4.2 billion euros of unpaid debts. Before that the company only fenced growing revenues and healthy profit margins. According to KPNQwest the bankruptcy was due to sudden drop in market prices. However research showed that even in the founding year the market price already plunged by 40 to 80 percent due to overcapacity and increased competition.	4.2 billion euros debt lost, in addition to lost stock value

Organization	**Cooks**	**Recipes**	**Incentives**	**Monitoring**	**End Results**

Innoconcepts	Top Management	Top management made the financial position of the company seem better by withholding debt from 10 Chinese organizations from the financial statements and from the external accountant. When the external accountant requested financial statements from the Chinese organizations they refused saying this was unusual in China. The external accountant is blamed for being okay with this, not investigating further and signing the financial statement. The management is also accused of trading with insider knowledge.	Hide true financial performance and self-enrichment.	The management is blamed for breaking corporate governance rules. The curator described the organizations management structure as incest. There were conflicts of interests between Innoconcept, her subsidiaries and the managements own private organizations. In addition the president-commissaries who was supposed to be the independent supervisor, actually did work for Innoconcepts. From this we conclude that there was a breach of segregation of duties.	Innoconcepts had an estimated market value of 400 million. The share price was 8 euro each share, which after the financial distress caused by the fraud dropped to 0.23 euro cents. In 2010 Innoconcepts was forced to file for bankruptcy. Because there was no cash available, the curator was unable to investigate. Investors lost most of their investment.

Organization	Cooks	Recipes	Incentives	Monitoring	End Results
Ahold	Top management	Subordinates overstated revenues by counting purchasing bonuses which were not met. Ahold Overstated revenues by withholding information from the external accountant. Ahold consolidated statements of subordinates in which they did not have a majority interests with their own. This is not allowed and is how Ahold could make their revenues seem higher for years.	Ahold had growth goals of 15% per year, the average growth rate in the branches was 1%. Large bonuses were tied to these high goals which caused management to commit fraud in order to achieve the goals.	The consolidation fraud is hard to detect because management created two contracts. The contract that was shown to the external auditor, said that Ahold had a majority interests and therefore consolidation was allowed. However the real contract was withheld from external accountants. The fraud from Aholds subordinates could have been detected earlier if Ahold had a centralized cash and treasury management in place By taking feeds from ERP systems and interfacing to external bank accounts, a centralized cash and treasury management system can deliver complete visibility of true cash flows in real-time, enabling discrepancies to be immediately identified. However such a system was not in place. The fraud eventually came to light by the new CEO, who started asking questions about the legitimacy of the notes.	Stocks go down with 63%. Fraud at US Foodservice (subsidiary) 880 million USD. Ahold pays investors back a total of 1.1 billion USD

In the next section the results of the case study and the interviews will be summarized in figures. The results on dangers to internal control systems are not summarized here because the answers did not allow for categorization.

Figure 11 shows that in 5 out of 10 cases top management was responsible for the fraud, two out ten cases middle management was responsible and in 3 out of ten cases top management was responsible.

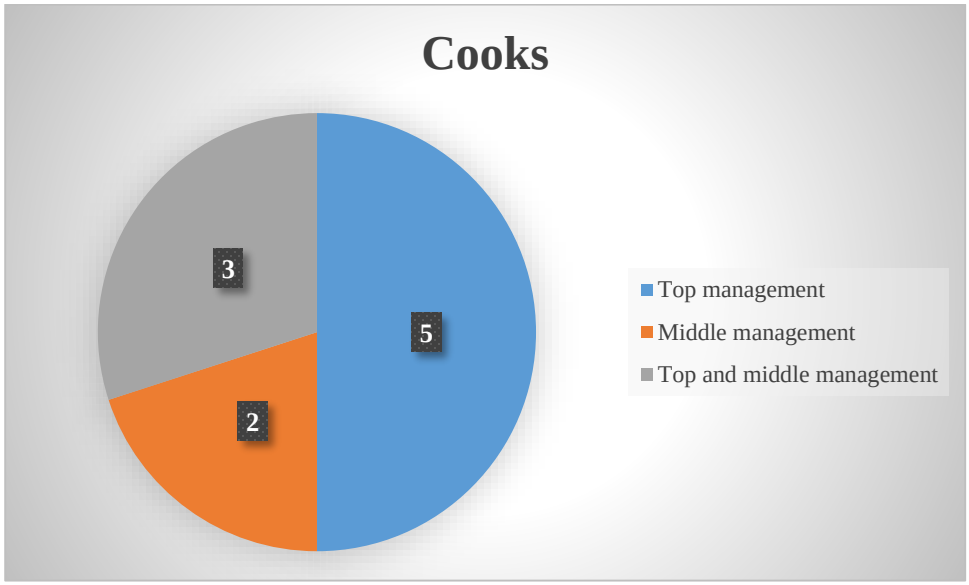

Figure 11: Cooks of financial statement fraud.

Figure 12 shows that in five cases false invoices were used as recipe, in four cases information was withheld, in 3 cases revenues were overstated and in two cases bribery was the recipe.

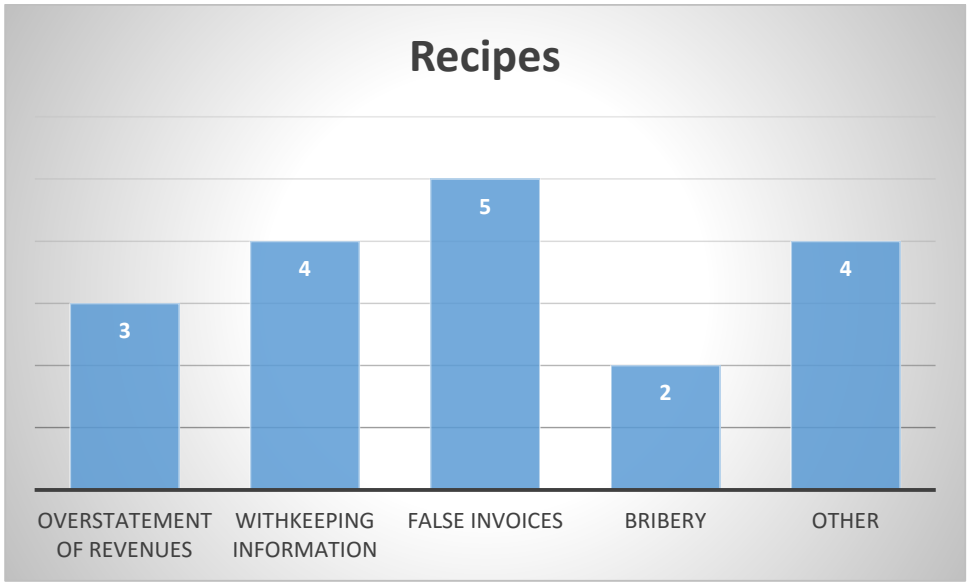

Figure 12: Recipe of financial statement fraud.

Figure 13 shows that self-enrichment is the incentive for committing fraud in five cases. Other incentives are improving organization performance (two cases), hiding performance (two cases), meeting goals (two cases), and excessive bonus culture (one case).

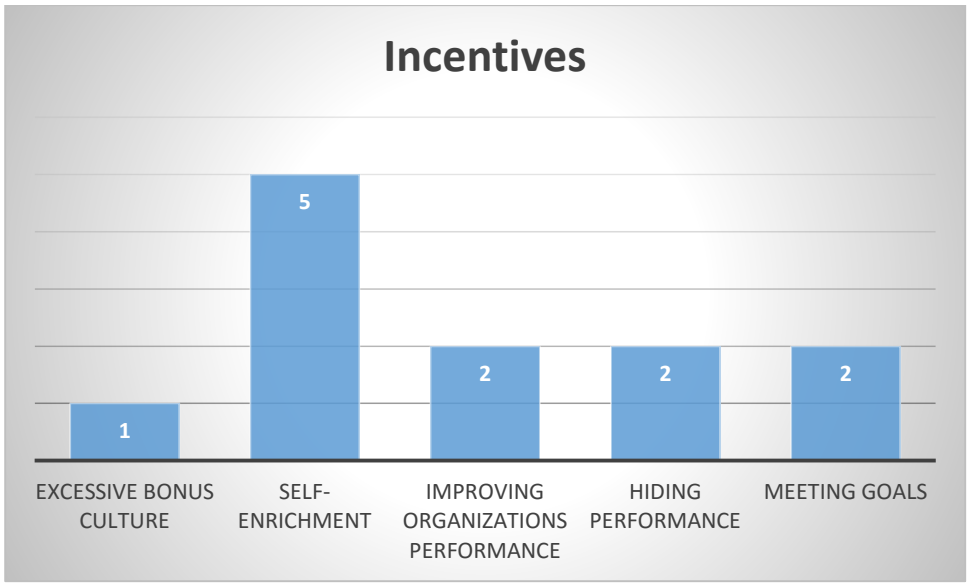

Figure 13: Incentives for committing financial statement fraud.

Figure 14 shows that in all cases management override was present. In seven cases in addition to management override, management also collided with one another. In two cases internal control systems were underdeveloped, in three cases poor segregation of duties lead to failure of internal controls. Last in two cases poor soft controls lead to the failure of internal control systems and in one case internal control detected the fraud but the money was already gone.

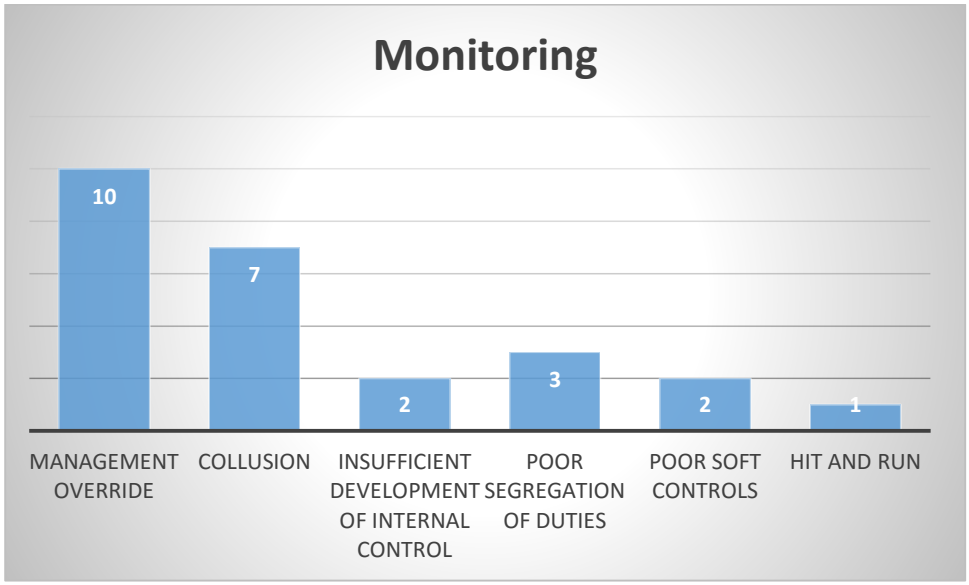

Figure 14: Monitoring of internal control

Figure 15 shows that in five cases the financial damage of internal control was over one billion, in three cases it was between ten million and one billion and in two cases it was less than ten million.

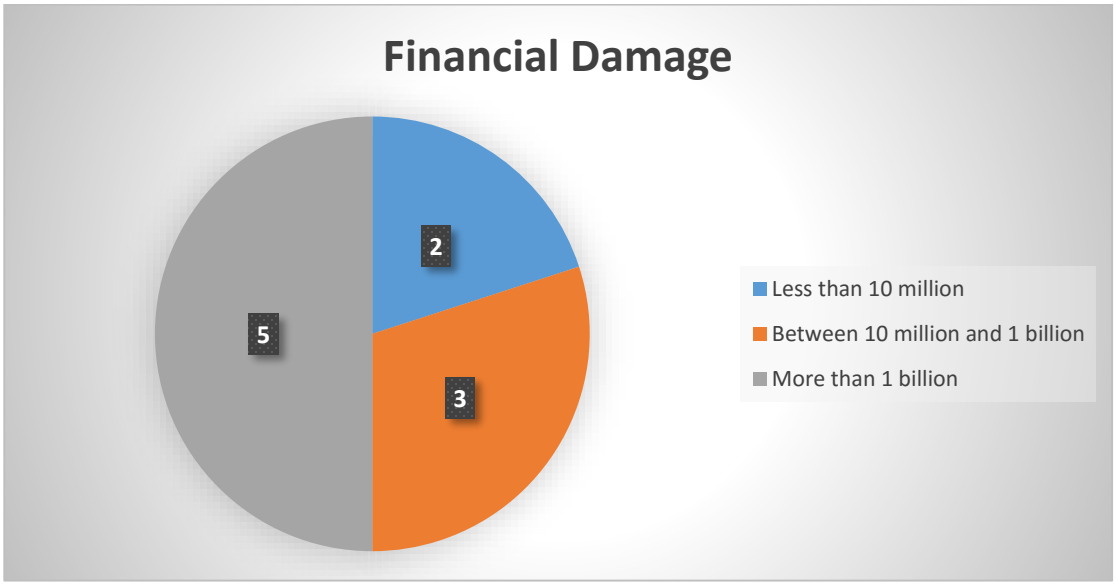

Figure 15: Financial damage of internal control.

Figure 16 shows best practices in fraud prevention, the right combination between hard and soft controls was brought up three times by different interviewees.

Figure 16: Best practices in fraud prevention.

Figure 17 shows that all interviewees agree that segregation of duties is the most important hard control, other important controls are the four eyes principle, visibility of internal controls and testing of internal control quality.

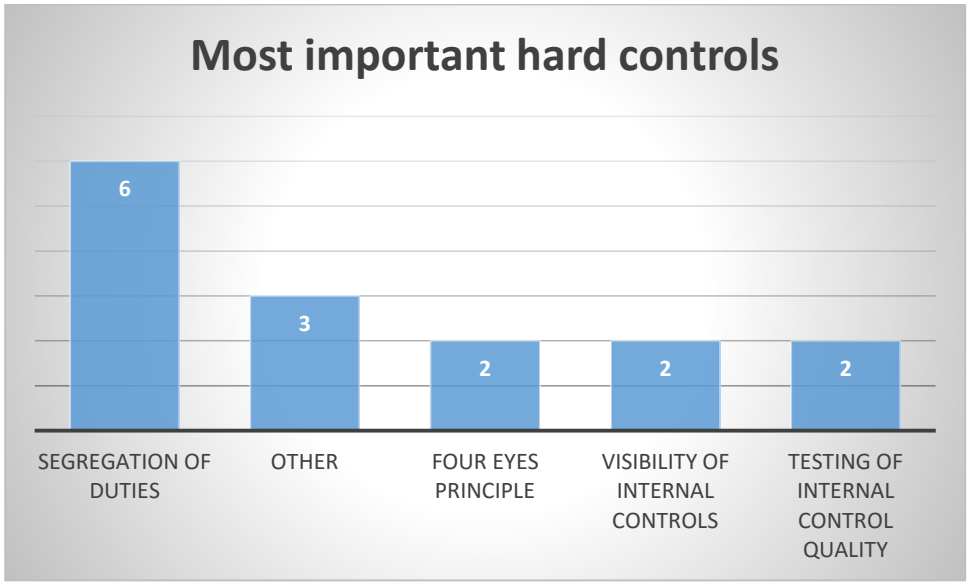

Figure 17: Most important hard controls in fraud prevention.

Figure 18 shows that risk analysis is deemed vital in creating efficient internal control systems by four out of six interviewees.

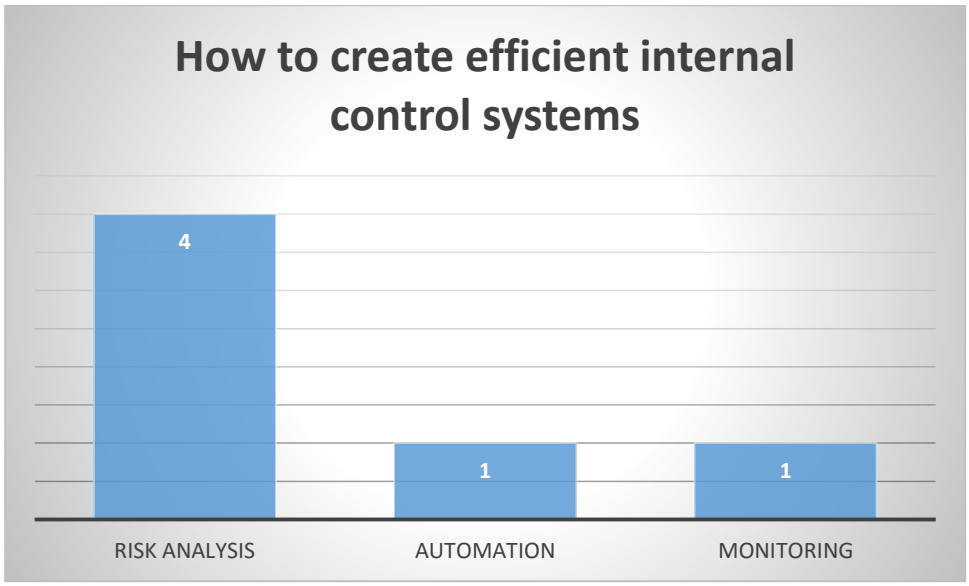

Figure 18: Efficient internal control systems.

Figure 19 shows that four of six interviewees think IT controls are an upcoming trend. Other upcoming trends in fraud prevention strategies are focus on soft controls and surprise checks.

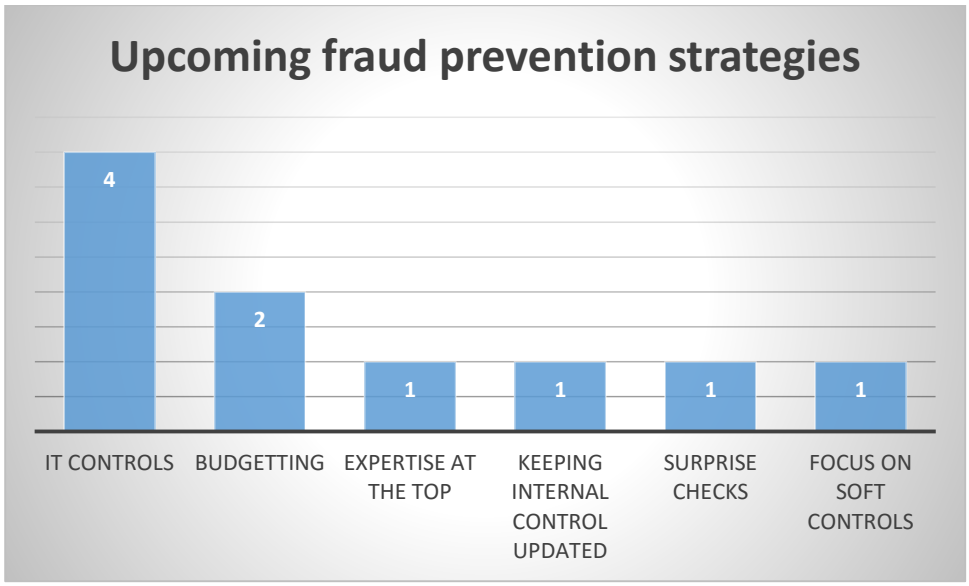

Figure 19: Trends in fraud prevention strategies.

Figure 20 shows that data analysis is the most important fraud detection tool. Other things that can help detect a fraud is insight in the organizations culture, and knowledge of the organization.

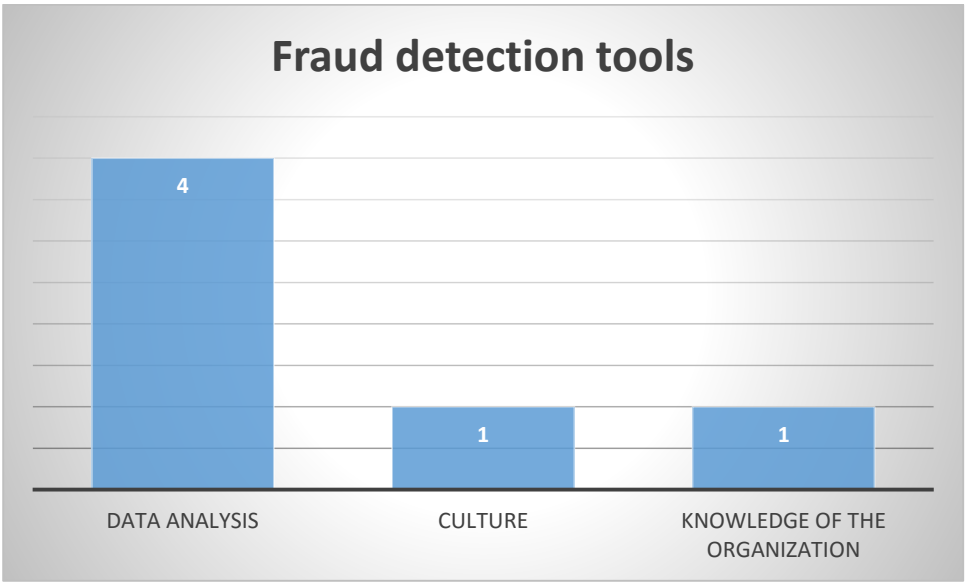

Figure 20: Fraud detection tools

Figure 21 shows the important of internal control. Most interviewees name the continuation of the organization as most important reason to invest in internal control. Other important reasons are prevention of fraud, securing external funding and providing assurance.

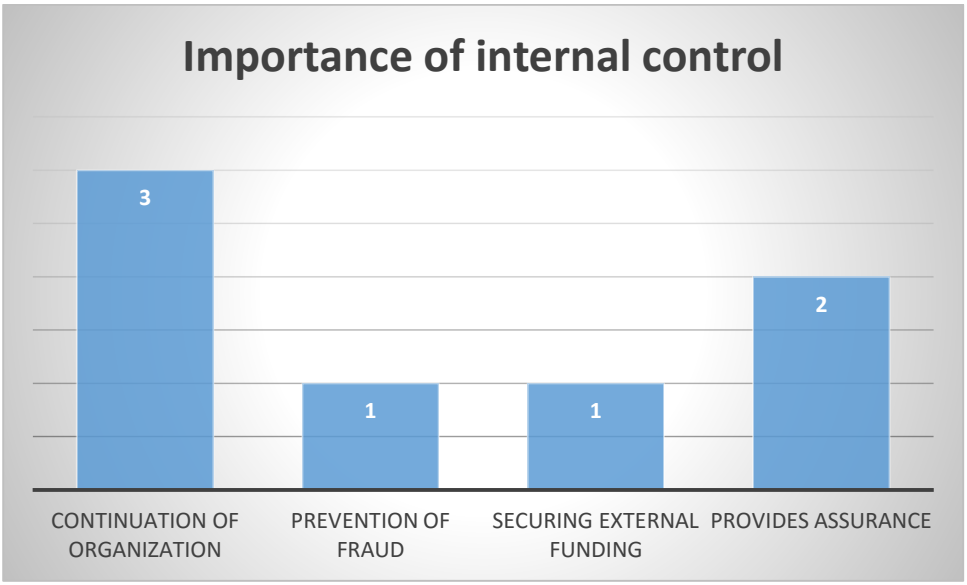

Figure 21: Importance of internal control.

We conclude that top management is usually responsible for committing financial statement fraud, using false invoices to hide it. Self-enrichment is the primary incentive for the fraudsters. In every case some form of management override is partly responsible for the failure of internal control, however management override is never the sole reason. Poor segregation of duties, fraud culture and/or collusion usually complement management override.

Best practice in creating an efficient internal control system is a good combination between soft and hard controls. Without proper soft controls, hard controls are inefficient. Other best practices are risk analysis, and having a good accountant. The most important hard control is segregation of duties. Other important hard controls are visibility of controls and the four eyes principle. Last it is important to check whether controls are actually complied with, and done properly. In order to increase internal control efficiency risk analysis is very important, organizations need to cover the right organization specific risks with the right controls. Automation of controls is an upcoming trend to further increase efficiency. Trends in fraud prevention strategy are IT controls. This works two ways, IT systems are becoming more complex thus requiring more controls. And IT systems offer more in the form of fraud detection by for example automating data analysis discovering anomalies. Data analysis is named to be the most important fraud detection tool, accountants look for anything out of the ordinary. An example is a booking out office hours. Last efficient internal control systems are reported to be vital for the continuation of the organization.

The interviewees and case studies confirmed or identified the following dangers to internal control systems: management override, collusion, weak culture, and financial distress. Management override is the most important danger, being present in every case and agreed by every interviewee. Collusion is present in seven out of ten cases, however interviewees seem to believe it does not happen often in fraud cases. Weak culture is identified by both the case study and the interviewees as a danger to internal control systems. Familiarization and the gain / loss principal were believed to be dangers to internal control systems by the interviewees, however only when the internal control system is not efficient. In addition to this the case studies do not show these dangers.

5 Discussion & conclusion

Although this research is qualitative that does not mean validity can be forgotten. To ensure validity of this research two actions have been undertaken. The first is doing a multiple case study. Studying ten cases made sure that results found over multiple cases are not on a one time basis. In addition to this expert interviews have been done with six employees of an accountancy/advisory firm. This means that results are not clouded by the judgment of one employee. Although six interviewees might not seem as much it needs to be noted that these employees have been employed at an accountancy/advisor firm for around ten years which means that they have worked for hundreds of organizations. However all six interviewees are employed at the same firm and in the same branch this may bias their opinions. For example respondents from different groups for example fraudsters might not share the same opinion.

The multiple case study has answered the first research questing by showing how fraud was committed at major Dutch organizations. It was shown that top management is usually responsible for committing financial statement fraud. Five out of ten cases top management was solely responsible for the fraud, in two out of ten cases middle management was responsible and in three out of ten cases it was a combination between top and middle management. Overstatement of revenues by using false invoices was the most popular recipe for fraud in five out of ten cases. Hiding information from third party is used in three out of ten cases. The recipes in the other two cases are bribery and reporting artificial revenues. Self-enrichment is the most important incentive for committing financial statement fraud in six out of ten cases. Other important incentives are hiding true performance, excessive bonus culture and meeting too ambitious goals. Management override made internal control systems less efficient in all cases. However there were weaknesses in internal control systems in almost all cases as well. In three out of ten cases the organization had a culture supporting fraud. In one organization a whistleblower even claimed fraud was in the DNA of the organization. In two out of ten cases there was no segregation of duties. One organization had a one man power structure, where the other organization had one manager who was responsible for the entire department. In four out of ten cases there was case of collusion, as shown in this research internal control systems simply cease to be effective when facing collusion. In the last case the organization simply grew too fast for internal control to keep up, meaning the organization no longer had control over its

expenditure. Financial damages were 4.5 billion (KPNQwest), 3.7 billion (SNS Reaal), 2.7 billion (Vestia), 2.5 billion (Imtech), 1.1 billion (Ahold), 400 million (Innoconcepts), 300 million (LCI Computer), 240 million (SBM Offshore), 4.5 million (Delta Lloyd), 2.5 million (Heineken). These findings on who committed the fraud, how, why, and what the result was are in line with the report to the nations on occupational fraud and abuse. This report includes 2410 cases of occupational fraud of which 5% in Western Europe (ACFE, 2016). Interestingly familiarization, gain/cost principal or financial distress have not come forward as reasons for the fraud in one of the cases, leaving management override, collusion and weak soft controls as the most important dangers to financial statement fraud. Management override and collusion were expected to be important, however soft controls like culture were not previously to the data collection.

The interview results provides more information on how accountants describe effective internal control systems, and their view on the dangers to internal control systems the second and third research questions. Internal control systems require a good mix between soft controls like culture and hard controls like segregation of duties. Some argue that soft controls are even more important, because when no one wants to commit fraud hard controls are not needed. To make internal control systems effective risk appetite and risk analysis are very important. First organizations need to decide how much risk they want to take, then map all the different organization specific risk and last organizations can decide what risks they want to cover. Excessive bonus policies are an incentive for employees to commit fraud, organizations should use such policies with caution. Segregation of duties and the four eyes principle are the most important hard controls. It is also important that controls are visible so third parties can rely on them. These findings are in line with what fraud prevention expert Rezaee has written in his book (2002).

Management override is considered to be the most important danger to internal control systems, and the biggest explanation when they fail. It renders internal control systems inefficient. However when organizations invest enough resources in soft controls the risk of management override can be reduced. Collusion causes internal control systems to fail. The risk of collusion can be minimalized by making sure no employee stays on the same job for too long. In addition to that culture is named to be effective, it is more difficult to find people to collide with in an organization that does not have a culture to support fraud. It is interesting that interviewees think collusion is rather uncommon, while the case study shows it happens in

almost every fraud case. For collusion and management override the results correspond with international literature (AICFE, 2005; Dorminey et al. 2012; Pfister, 2009; AICPA, 2005). Financial distress provides incentive to commit fraud, this can be mitigated by focusing on soft controls and automation of as many controls as possible. This also corresponds with international literature (Dorminey et al, 2012). However for familiarization and the cost gain principle the results do not correspond. Neither dangers to internal control systems were shown in the case study. In addition to that the interviewees have their doubts about each of the dangers. When familiarization exposes weaknesses in the internal control systems, then they were not created properly in the first place. While the cost gain principle could lead to less effective internal control, organizations can solve this problem by deciding on their risk appetite and mapping all the organization specific risks (Kinney, 2002; Dorminey et al, 2012). This explains the use of both research methods interviews and multiple case studies. Because it identifies discrepancies between the two. While interviewees believed collusion to be dangerous to internal control system they also believed it was not common, while the case study shows that it is in fraud cases. Another discrepancy is that the interviewees believe that the gain/loss principal and familiarization dangers are both easily minimized. Concluding it can be stated that management override and collusion are the biggest dangers to otherwise effective internal control systems, the best way to minimize these threats is to focus on soft control. Thus organizations can create an environment in which internal control systems can be effective in preventing financial statement fraud.

Due to time and availability constraints this research has some limitations. Because the research focused on ten large cases of financial statement fraud the findings are generalizable to these cases only. For example smaller fraud cases might be committed by lower management instead of top management. In addition as gathering primary data for the case study would absorb too much time secondary data was used. This data is subject to the bias of the author that provided the secondary data. The interviewees all worked for the same firm which may bias their opinions. In addition to this four out of six interviewees filled senior management vacancies which may bias their opinions. For example the importance of soft controls will probably be highlighted by higher management because they have more to do with soft controls in their daily work. Last all interviewees worked in the accountancy branch, four directly and two in advisory

roles. Although this provides a good accountancy point of view, it leaves out the view of other groups that could be just as important. Examples are the fraudster or the victim.

This research aimed to explain why internal control systems failed in preventing financial statement fraud. It found a couple of explanations. However the results are qualitative, it would be interesting to test these explanations to a larger data set. An example of such a study is the global survey done by ACFE (2016), but instead focused on the Netherlands. Another interesting study could research how to best prevent or detect management override and conclusion, the biggest dangers to internal control systems. While this research provided some advice it is based on six interviewees working in the accountancy branch, it could be interesting to see how fraudsters or organizations would minimize these threats. Last this study has shown that false invoices is the most common method for hiding financial statement fraud, thus organizations are in need of scientific research on how to prevent false invoices.

The practical implications of this study are that internal control systems are an effective fraud prevention method. The two most important dangers are management override and collusion. The risk of management override can be minimized with proper segregation of duties. However even when that is the case management can collide with each other to commit financial statement fraud. Therefore it is important for organizations to have a proper combination between the right hard controls and the right soft controls. The soft controls are there to minimize the risk of management collusion. It is harder to collide with people in an organization with an anti-fraud culture.

References

Albrecht, W. S. (2006). *Fraud Examination.* New York: Thomson South-Western.

Albrecht, W. S., Howe, K. R., & Romney, M. B. (1984). *Deterring fraud: the internal auditor's perspective.* Altomonte Springs: The Institute of Internal Auditors' Research Foundation.

Algemeen Nederlands Persbureau. (2010). Zwarte celfstraf voor fraudezaak Delta Lloyd. Retrieved from http://www.nu.nl/nuzakelijk-overig/2403433/zware-celstraf-fraudezaak-delta-lloyd.html

Algemeen Nederlands Persbureau. (2017). Celstraf geëist voor miljoenenoplichting Delta Lloyd. Retrieved from http://www.nu.nl/binnenland/2388283/celstraf-geeist-miljoenenoplichting-delta-lloyd.html

American institute of certified public accountants. (2005). *Management override of internal controls: the achille's heel of fraud prevention.* New York: AICPA.

Association of Certified Fraud Examiners. (1995). *Cooking the books: what every accountant should know about fraud.* Austin: TX.

Association of certified fraud examiners. (1996). *Report to the nation on occupational fraud and abuse.*

Association of certified fraud examiners. (2008). *Report to the Nation on Occupational Fraud and.* Austin: ACFE.

Association of certified fraud examiners. (2009). *Fraud examiners manual.* Austin: ACFE.

Association of certified fraud examiners. (2012). *Report to the nations on occupational fraud and abuse.* Austin: ACFE.

Association of certified fraud examiners. (2016, September 26). *Report to the nations.* Retrieved from ACFE: https://s3-us-west-2.amazonaws.com/acfepublic/2016-report-to-the-nations.pdf

Beasley, M. S., V, C. J., & Hermanson, D. R. (2010). *Fraudulent Financial Reporting 1987-1997: An Analysis of U.S. Public Companies.* Committee of Sponsoring Organizations of the Treadway Commission.

Bell, T. B., & Carcello, J. V. (2000). A decision aid for assessing the likelihood of fraudulent financial. *Auditing: A Journal of Practice & Theory*, 169–184.

Breton, G., & Taffler, R. J. (2001, September 26). Accounting information and analyst stock recommendations: a content analysis approach. *Accounting and Business Research*, 92-101.

Canadian Institute of Chartered Accountants. (1995). *Guidance on control.* Toronto: COSO.

Cohen, D. A., Dey, A., & Lys, T. Z. (2007). Real and Accrual-based Earnings Management in the Pre- and PostSarbanes. *The accounting review*.

COSO. (1999). *Report on fraudulent financial reporting.* COSO: New York.

COSO. (2013). *Internal control-integrated framework.* New York: COSO.

Cressey, D., & Sutherland, E. H. (1992). *Principles of criminology.* Lanham: AltaMira Press.

Cressey, R. D. (1950). The criminal violation of financial trust. *American Sociological Review*, 738–743.

Cressey, R. D. (1953). *Other People's Money: The Social Psychology of Embezzlement.* New York: The Free Press.

De Heus, R. S., & Stemmelaar, M. T. (2000). *Auditen van soft controls.* Deventer: Kluwen.

De Kort, J., & Elst van der, C. F. (2014). Corporate Governance: De verhouding tussen 'hard- en soft controls' in de Nederlandse bestuurskamer. *Tilburg University*.

Dorminey, J. A., Fleming, S. A., Kranacher, M.-J., & Riley, R. A. (2012). The evolution of fraud theory. *Issues in accounting education*, 555-579.

Eisenhardt, K. (1989). Agency theory: An assessment and review. *Academy of management review*, 57-74.

Ernst and Young. (2003). *Fraud - the unmanaged risk: An international survey of the effect of fraud on business.* London: Ernst and Young.

Financieel Dagblad. (2016). Boekhoudfraude Mitra nekte drankengroep dirkzwager. Retrieved from https://fd.nl/ondernemen/1177160/boekhoudfraude-mitra-nekte-drankengroep-dirkzwager

Flick, U. (2011). *Introducing research methodology.* London: Sage.

Fraude. (2015`). *Van Dale.* Utrecht: VBK Uitgevers.

Gao, L., & Srivastava, R. P. (2011). The anatomy of management fraud schemes: analysis and implications. *Indian accounting review*, 1-20.

Giebels, R. (2015). Bestuurders vastgoedtak SNS Reaal voor de rechter. Retrieved from http://www.volkskrant.nl/economie/bestuurders-vastgoedtak-sns-reaal-voor-de-rechter~a4177456/

Glaser, B. G., & Straus, A. (1967). *The discovery of grounded theory: strategies for qualitative research.* New York: Aldine.

Golden, T. W., Skalak, S. L., & Clayton, M. M. (2006). *A guide to forensic accounting investigation.* London: John Wiley & Sons.

Griffiths, I. (1986). *Creative Accounting.* London: Sidgwick and Jackson.

Gualthérie van Weezel, T. (2016). Retrieved from http://www.volkskrant.nl/economie/om-vervolgt-zeven-verdachten-wegens-vestia-schandaal~a4312365/

Gullkvist, B., & Jokipii, A. (2013). Perceived importance of red flags across fraud types. *Critical perspectives on accounting*, 44-61.

Herriott, R. E., & Firestone, W. A. (1983). Multisite qualitative policy research: Optimizing description and generalizability. *Educational Researcher*, 14-19.

Hogan, C., Rezaee, Z., Riley, R., & Velury, U. (2008). Financial statement fraud: Insights from the academic. *Auditing: A Journal of Practice & Theory*, 27.

Jones, M. (2011). *Creative accounting, fraud and international accounting scandals.* Chichester: John Wiley & Sons.

Kaptein, M., & Wallage, P. (2010). Assurance over gedrag en de rol van soft controls: een lonkend perspectief. *Maandblad voor accountancy en bedrijfseconomie*, 623-632.

Kasteleyn, P., & Vrijbloed, R. C. (2006). Boekhoudfraude bij Ahold. *Controllers*, 15-17.

Kimmel, P. D., Weygandth, J. J., & Kieso, D. E. (2011). *Financial Accounting.* Wiley.

Kinney, W. R. (2000). Research opportunities in internal control quality and quality assurance. *Audit Journal Practising Theory*, 83-90.

KPMG. (2007, October 26). *Cross-border investigations, effectively meeting the challenge.* Retrieved from http://www.kpmgvergi.com/PDF/Yayinlar/KPMG-Global-Yayinlar/Cross-Border-Investigations-Effectively-Meeting-the-Challenge.pdf

KPMG. (2012). *Fraud and Misconduct Survey.* Retrieved December 15, 2016, from http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Documents/fraud-bribery-corruption-survey-2012.pdf.

KPMG. (2016, Februari 1). *Acht basis soft controls.* Retrieved from Assets KPMG: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/20160218-acht-basis-soft-controls.pdf

Kranacher, M. J., Riley, R. A., & Wells, J. T. (2011). *Forensic Accounting and Fraud Examination.* New York: John Wiley & Sons.

Krishnan, J. (2005). Audit committee quality and internal control: An empirical analysis. *The accounting review*, 649-675.

Libbenga, J. (2016). Heineken leeggetrokken door fraudeurs. Retrieved from https://www.sprout.nl/artikel/heineken-leeggetrokken-door-fraudeurs

Maijoor, S. (2000). The internal control explosion. *International Journal of Auditing*, 101-109.

Merchant, K. (1985). *Control in business organizations.* Marshfield: Pitman Publishing.

Monitoring Commissie. (2016). *Corporate Governance Code.*

Mulford, C., & Comiskey, E. (2002). *The financial numbers game, detecting creative accounting practises.* New York: John Wiley & Sons Inc.

Nederlandse omroep stichting. (2015). Klokkenluider SBM Offshore doet boekje open over corruptie. Retrieved from http://nos.nl/nieuwsuur/artikel/2017267-klokkenluider-sbm-offshore-doet-boekje-open-over-corruptie.html

Nods, R. (2015, August 11). Hoe een gebrek aan controle imtech wist te nekken. *Elsevier*. Retrieved from http://www.elsevier.nl/economie/article/2015/08/hoe-een-gebrek-aan-controle-imtech-wist-te-nekken-2669835W/

OECD. (2004). *Principles of corporate governance.* Paris: OECD.

Olsthoorn, P. (2010). KPNQwest was gewoon een criminele organisatie. Retrieved from http://www.netkwesties.nl/298/kpnqwest-was-gewoon-criminele-organisatie.htm

PCAOB. (2007). *Auditing standard no. 5: An audit of internal control over financial reporting that is integrated with an audit of financial statements.* Public Company Accounting Oversight Board.

Pfister, J. A. (2009). *Managing organizational culture for effective internal control: from practise to theory.* Dordrecht: Springer.

PWC. (2011). *Cybercrime: Protecting against the growing threat.* London: PWC.

Rezaee, Z. (2005). Causes, consequences, and deterence of financial statement fraud. *Critical Perspectives on Accounting*, 277-298.

Rezaee, Z., & Riley, R. (2011). *Financial statement fraud: prevention and detection.* New Jersey: John Wiley & Sons.

Robertson, J. C. (2000). *Fraud examination for managers and auditors.* Austin: Viesca Books.

Schuchter, A., & Levi, M. (2015). Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum*, 176-187.

SEC. (2007). *Management's report on internal control over financial reporting.* Washington DC: Securities Exchange Comission.

Simons, H. (2009). *Case study research in practise.* London: Sage.

Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal.* Boston: Harvard Business School Press.

Stolowy, H., Messner, M., Jeanjean, T., & Baker, C. R. (2013). The Construction of a Trustworthy Investment Opportunity: Insights from the Madoff Fraud. *Contemporary Accounting Research*, 1-62.

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review*, 1-12.

Thomas, G. (2011). *How to do your case study.* London: Sage.

Usman, A. K., & Shah, M. H. (2013). Critical succes factors for preventing e-banking fraud. *Journal of internet banking and commerce, 18*(2).

Vereniging van effectenbezitters. (2009). De duurste pen ter wereld, fraude en gedupeerde beleggers. Retrieved from https://www.veb.net/artikel/01588/de-duurste-pen-ter-wereld-fraude-en-gedupeerde-beleggers

Vereniging van effectenbezitters. (2015). Curator ongekend hard over wantoestanden bij failliet Innoconcepts. Retrieved from https://www.veb.net/artikel/05629/curator-ongekend-hard-over-wantoestanden-bij-failliet-innoconcepts

Vink, H. J., & Kaptein, M. (2008). Soft controls bij de rijksoverheid: Een onderzoek naar de oorzaak van rechtmatigsheidfouten. *Maandblad voor accountancy en bedrijfseconomie*, 256-264.

Wolfe, D. T., & Hermanson, D. (2004). The Fraud Diamond: Considering the four elements of fraud. *The CPA Journal*.

Yadav, B. (2013). Creative accounting: A literature review. *The SIJ Transactions on Industrial, Financial & Business Management*.

Yin, R. K. (2003). *Case study research design and methods.* Thousand Oaks: Sage Publications.

Appendices

A Examining the risk of financial statement fraud using the fraud triangle

This checklist shows the possible weaknesses of internal controls, as well as general variables that have an effect on the risk of financial statement fraud. The checklist is based on the fraud triangle in that it divided different variables in groups on which they have most effect: Pressures (incentives and motives), opportunities, and attitudes and rationalizations.

Pressures

1. Is the organization financially stable or is their profitability unstable?
    a. Level of competition
    b. Level of saturation
    c. High or low margins
    d. Speed of industry change
        i. Technology
        ii. Threat of substitute products
        iii. Interest rates
    e. Change in customer amount
    f. Amount of defaults / bankruptcies in Industry
2. Is the organizations financial performance in line with industry expectations?
    a. Unusual growth rate
    b. Unusual profitability
    c. Unusual financial results
3. Does the organizations financial stability or profitability show signs of weakness?
    a. Operating losses
    b. Negative cash flow from operations
    c. Positive earnings and earnings growth in combination with negative operating cash flow
4. Is there excessive pressure on management to meet expectations in following statements?
    a. Press releases
    b. Annual reports

   c. Forecasts
   d. Communications with other parties
5. Does the organization require more debt or equity for the following processes?
   a. R&D
   b. Capex
   c. Salaries
   d. Account payable
   e. Debt
   f. Debt covenants
6. Does reporting bad financial results have a direct influence on following transactions according to management?
   a. Credits
   b. New equity
   c. Mergers
7. Do managers have personal interest in the organizations?
   a. (Partial) ownership
   b. Compensation through:
      i. Bonus
      ii. Salary
      iii. Stock options
      iv. Other arrangements
   c. Personal debt in the organization
8. Are there any indications of earning management at lower levels?
   a. Pressure on low level management
   b. Idea of low management that reporting bad results leads to negative consequences

Opportunities

1. Does the nature of the organization give opportunity for financial statement fraud?
   a. Related party transactions
   b. Organization is able to dictate terms to suppliers/customers
   c. Important estimates require subjective judgment

   d. Transactions that are highly complex
   e. International operations
   f. Operations in tax haven
   g. Changes to accounting system
   h. Mergers and acquisitions
2. Indications that estimates used in financial statements are:
   a. Unrealistic
   b. Inconsistent with history, industry, past communications
3. Evidence of management override:
   a. Domination by single person or group
   b. No oversight financial reporting / internal controls
   c. Turnover is unreasonably high of senior management
4. Complex or unstable organizational structure:
   a. Difficult to identify ownership
   b. Legal entities present are unusual
   c. Lines of authority are unusual
5. Inefficient internal controls
   a. Monitoring is inadequate
   b. Fraud risk assessment is inadequate
   c. Identification of business risk fails
   d. Failed monitoring of identified business risks
   e. High turnover accounting staff
   f. Incompetent accounting staff

Attitudes and rationalizations

1. No evidence of appropriate tone at the top:
   a. Unclear values and ethical standards
   b. Inappropriate values / ethical standards
   c. Unwilling to fix financial statement or disclosures
   d. Attitude against antifraud programs and controls
2. Abnormal occupation with:

   a. Accounting principles
   b. Estimates
   c. Stock price
   d. Growth
   e. Minimizing earnings for tax reasons
3. History of violations of:
   a. Securities laws
   b. Other laws
   c. Regulations
4. Any pending claims against the organization?
5. Failure to correct known internal control failures?
6. Repeated attempts to justify inappropriate materiality?
7. Strained relationship with ex auditor?

(Rezaee & Riley, 2011) (American institute of certified public accountants, 2005)

B Interview invitation

Interview: The role of internal accounting controls in preventing and detecting Dutch financial statement fraud.

The research investigates the effect of internal control systems in preventing financial statement fraud committed by top management in the Netherlands. Recently there have been a few major cases of financial statement fraud in the Netherlands: OGEM (1970-1979), RSV (1975-1979), Fokker (1988), Baan Company (1997), Landis (1999-2001), LCI Computer (1999-2001), Royal Ahold (1999-2002), Van der hoop (2005), Vestia, SNS Reaal, Imtech and Innoconcepts (2010). The research aims to explain why internal control systems have failed in aforementioned cases, and how a system can be created that is more capable of preventing financial statement fraud. With internal control system we mean the hard controls, examples of this are: segregation of duties and the four-eye principal. Financial statement fraud is when an organization deliberately gives a misstatement to mislead internal and external parties like banks, shareholders and contract holders. Organizations names will not be given nor will organizations be described in this thesis.

Introduction:

1. Are you okay with this conversation being recorded?
2. Are there any questions about the research before we start the interview?
3. Can you describe your current employment?
4. Can you describe how you come in contact with internal control systems during your work activities?

Research questions:

Fraud prevention strategies:

5. In your experience what are best practices in preventing financial statement fraud?
6. In your experience what are the best controls an organization should have in place for preventing financial statement fraud?
7. What is required for an efficient internal control system?
8. What are current fraud prevention strategies?
9. What are strengths and weaknesses of internal control systems?

10. What tools does an organization have to detect fraud?

Dangers to internal control systems:

11. In your experience what is the effect of management override on internal control systems, and how can that effect be minimalized?
12. In your experience what is the effect of collusion on internal control systems, and how can that effect be minimalized?
13. In your experience what is the effect of familiarization on internal control systems, and how can that effect be minimalized?
14. In your experience what is the effect of the gain/loss principal on internal control systems and how can organizations find the quality optimum?
15. What do you advise organizations that are in financial distress in relation to internal control systems?
16. In your experience, are there any other dangers to internal control systems that were not mentioned?

Practical fraud case (optional):

17. Do you have a personal experience with financial statement fraud? If yes, can you describe this case, explain how it came to light, and how according to you it could have been prevented or detected earlier?

C Interview transcripts

Interview: A
Date and time of interview: 06-02-2017

Interviewee: Audit partner

Introduction:

1. Are you okay with this conversation being recorded? **Yes**
2. Are there any questions about the research before we start the interview? **No**
3. Can you describe your current employment? **Audit Partner**
4. Can you describe how you come in contact with internal control systems during your work activities?

In relation to the audit of the yearly financial statement we check the administrative organization. In our function we check for weaknesses in internal control and which activities we should undertake in relation to these weaknesses.

Research questions:

Fraud prevention strategies:

5. In your experience what are best practices in preventing financial statement fraud?

It is necessary to have multiple checks, and a good accountant. I think it is very important to have conflicting interests in an organization, the financial department should not do everything by themselves, but the CEO/Commercial department should tune with the financial department about the financial statement. The risk is greater when the financial department is solely responsible for the financial statement. The responsibility should lie with all departments, other departments should ask themselves does this make sense and do we support this statement.

6. In your experience what are the best controls an organization should have in place for preventing financial statement fraud?

Visible separation of duties. One party should take responsibility and the other should observe. Visibility means its observable for a third party like the external accountant. In addition you want the quality of internal controls to be tested. For example by seeing if a control was actually done, however you want to go to a higher level in which you test if multiple controls worked properly. A margin check is an example of an overarching control. In practice controls are often in place, but are not visible. Organizations should realize that they do not do this for the

accountant but for themselves. Concluding the best internal control are separation of duties and visibility, what has been done?

7. What is required for an efficient internal control system?

Efficiency and internal control is something that can bite. Some customers are fine as long as it doesn't increase their costs, this proves to be difficult. You have to invest in internal controls with wit. We check with customers where are the risks, how to get money out of this organization? What kind of products do you have? Are they tradable? When the product is not tradable the biggest risk is money being stolen. Cash money is not an issue anymore this was earlier. No payments are done in cash today this limited the possibilities. It goes wrong when someone controls departments, for example does both the sales and the purchasing. There has to be breach of separation of duties. When separation of duties, the payments organization are in order and your products are not tradable it is very difficult to commit interesting fraud. Too much trust in an organization is not good for preventing fraud.

8. What are current fraud prevention strategies?

In the Netherlands we focus on separation of duties, you also see that IT is coming up. Products are being made that are able to analyze data from ERP systems to find breaches in the internal control system. We also see period reporting, monitoring and budgeting, if it works properly these are good prevention strategies but often they do not.

9. What are strengths and weaknesses of internal control systems?

When we do clients for the first year, we check soft controls. This is very much about the tone at the top, what kind of example does top management set. This is needed to say anything about the working of hard controls. An example of this is during a SOX control, which required a signature on everything. The signature was set but the culture was so that it was not actually checked. This is a case of the right hard controls, but due to bad soft controls (culture) they did not work. Internal control is not so much about strengths/weaknesses but it is mandatory, an organization cannot exist without internal control. Advantages are earlier detection and prevention of problems. A weakness of internal control is when separation of duties is breached and when the interests become too big. For example an excessive bonus system weakens the internal control system. As auditors we always check bonus agreements.

10. What tools does an organization have to detect fraud?

In our control we aim at prevention. Detection is in strange things, we check trends and numbers for remarkable cases. And increasingly more data analysis. For example when bookings take place, is it during the day or in the evening and who did the booking. It is out of the ordinary when a CFO who should not even do bookings himself, does a booking out of office hours. Best would be if CFO would not even be able to do bookings. An auditor has to think with the mindset of a fraudster, this is discussed with the customer. For example I ask him if you wanted to get money out of this organization, how you would do it. However if the customer the fraudster they will obviously have an answer ready but it can show weaknesses in internal control.

Dangers to internal control systems:

11. In your experience what is the effect of management override on internal control systems, and how can that effect be minimalized?

This is a very logical risk. In our financial statement control this is also a standard risk. But it depends on the nature of the organization and the height of rewards. The height of salary can be an indicator for management override. For example when employees are getting paid more than they would elsewhere, they are less likely to stand up to their managers when asked to do something that contrasts with internal control. The greater your own interest is the more likely you are to go along with whatever your supervisor says. An organization that has very pushy auto reactive, management has a higher risk of financial statement fraud than an organization that leaves responsibilities with their employees.

12. In your experience what is the effect of collusion on internal control systems, and how can that effect be minimalized?

Collusion is really hard for us to detect. However when accountants constantly ask themselves how can I gain from this, how can I get money out of this organization even collusion can be hard to commit. The problem is that you have to trusts each other a lot as you commit a felony together. In professional environments I do not see this a lot. However in small organizations the risk is higher. An example is two salesmen that work together in a store for multiple years, complaining about how their boss is constantly playing golf. These people bond and are eventually able to rationalize their crime. Concluding it is hard for us to detect, but in larger organizations the risk is low. The fraud triangle is used when we discuss the possibilities for

fraud in the team, it is mainly use for detection of fraud risk factors. This is a very creative part of the accounting job. This is the reason it is very important, to fully understand the customer, how does the sales process work, how do you work with agents, how do bonus agreements work?

13. In your experience what is the effect of familiarization on internal control systems, and how can that effect be minimalized?

I don't see this very often. Internal control systems are not stable. If you compare to 5-6 years ago the power of ERP systems has increased tremendously. In a stable environment this would be a risk, but we don't see it very often. I also think it's not as possible, our controls are not aimed to this risk. The only way I would think the risk would become greater is when one employee is responsible for the same job for a long amount of time. For example a purchaser of used cars, who both buys and sells. However this is a real exception. Another risk is that of a purchaser that is in the same place for a long time, you can get the contract for the office garden, if you also do my home garden. Therefore we check whether offers have been asked from at least three suppliers.

14. In your experience what is the effect of the gain/loss principal on internal control systems and how can organizations find the quality optimum?

I think it depends on a lot of things. The risk increases when you are in financial distress. Cost savings, reorganizations, firing employees but still having to comply with bank covenants. There is no rule for investing in internal control, it really depends on the organization.

15. What do you advise organizations that are in financial distress in relation to internal control systems?

I would advise to see where we can cut. It might sound weird but the soft controls are more important than the hard controls in my opinion. If the soft controls are working properly hard controls are in theory not really needed. Of course in practice you need the combination. Save on hard controls where possible, less period reports but keep investing in soft controls.

16. In your experience, are there any other dangers to internal control systems that were not mentioned?

When the internal control system is not sufficient, than the risk of errors in the financial statement increases. However this the focus of your research is deliberate misstatement. Of previously named dangers management override is by far the most dangerous. I see no others.

Practical fraud case (optional):

17. Do you have a personal experience with financial statement fraud? If yes, can you describe this case, explain how it came to light, and how according to you it could have been prevented or detected earlier?

I have a management fraud. We were called by the organization that the previous director was not paying taxes for his lease car. This was an indicator for us that more may have been going on. Therefore we reevaluated the organization together because this said something about the tone at the top. This did not lead to any self-enrichments frauds, however did find a fraud that profited the organization. By selling goods that were written off outside the books. The accountant was fooled thinking they were incinerated, and no taxes were paid. This was detected by talking to the factory supervisor.

Interview: B
Date and time of interview: 8 February 2017 13:00-14:00

Interviewee: Risk consultant

Introduction:

1. Are you okay with this conversation being recorded? **Yes**

2. Are there any questions about the research before we start the interview? **No**

3. Can you describe your current employment? **Senior manager, Risk consultant**

4. Can you describe how you come in contact with internal control systems during your work activities?

Our goal is to go to the market convincing organizations that they can have better internal control. Too show them best practices and to share the experience we obtain serving our different clients. Or too help clients with specific questions about fraud risk control.

Research questions:

Fraud prevention strategies:

5. In your experience what are best practices in preventing financial statement fraud?

I think many organizations insufficiently map the specific risks that are applicable to their organization. These risks can be strategic, operational, financial or compliance. Fraud is mostly in the operational, financial and compliance corner, not so much in the strategic. Most of the time there is a yearly meeting about risk control, to see whether risks that were applicable last year are still this year. Without talking about what is coming at us, what is going on in the branches, law and regulations that change. Without this information it is impossible to create a strong internal control system. Risks can be both internal and external, an example of an internal risk is culture and behavior. I think this is a risk that is underexposed. This is shown in the new corporate governance code that emphasizes the culture element. Management is responsible for implementing the right culture within the organization.

6. In your experience what are the best controls an organization should have in place for preventing financial statement fraud?

Segregation of duties is a minimal requirement. The four eyes principal. And a good mix between preventive controls and detective controls. You shouldn't have only detective controls at the end of a process. But you should also have preventive controls. When for example you have the purchasing process, it is common to have the controls and the end of the process.

When is the payment, when is the accountability? And to little controls at the beginning of the process, do I control my master data? My suppliers? Approval of purchasing orders? Is it recorded and monitored? Registered properly? During the entire process you should ask yourself, where can something go wrong? What do I see as the most important risks? Because you can also do too much for example 100 controls per process. What are my key controls and what are my key risks within this process?

7. What is required for an efficient internal control system?

An efficient control system starts with establishing what are the risks that are important to my organization? Larger organizations are pragmatic, it should not cost too much. Smaller organizations often ask we are a small organization, what are the minimal requirements to comply? I think this is a very wrong mindset. You should create a good internal control system in which you cover the right risks with the right controls to create an optimal mix and efficient internal control system. Too make the system efficient I would try to automate as much as possible controls. Automation is an upcoming trend, an example are ERP Systems. Another addition is data analysis done by accountancy firms. In order to recognize weird patterns or double invoices. One example is to check the bank accounts of your employees and the bank accounts of your suppliers, sometimes you come across weird cases. It can happen you come across the bank account number of one of your employees on the bank statement of your supplier, naturally this should sound alarm bells.

8. What are current fraud prevention strategies?

There is more and more attention for general IT controls around your ERP systems. A question is who has access to what parts of your financial systems? This is called access management. Another strategy is realistic budgeting, an example of how this can go wrong is Japan. Pressure from shareholders who expected unrealistically high revenues created an optimized setting for fraud. Expertise at the top is another strategy, for example in a major Dutch fraud case it came to light that almost no one had sufficient knowledge of financial instruments.

9. What are strengths and weaknesses of internal control systems?

Internal control system are a synergy between multiple components. Your risk assessment is the basis of internal control. After that your control activities follow, which information do I need to cover those risks? It is about finding the right mix between several levels, you will

need all controls. On lower levels in the organizations you need transactional controls like approval of invoices and declarations of employees.

10. What tools does an organization have to detect fraud?

When our colleagues investigate an organization for fraud they check for culture but also for organization specific fraud risks. An auditor but also an organization self should ask what fraud risks that I think are relevant are and I would like to control for.

Dangers to internal control systems:

11. In your experience what is the effect of management override on internal control systems, and how can that effect be minimalized?

The effect of internal control is that either way they are circumvented or employees are pressured into complying to do things not or not properly or in a way that it seems proper but actually is not. For example payments without any support. How can we prevent this? I Think culture and behavior is really important, this sort of practices should not be desirable. There should be a whistleblower program, and it should be very clear within the organization where to report possible frauds. I think these two are the most important.

12. In your experience what is the effect of collusion on internal control systems, and how can that effect be minimalized?

You can create an internal control system that's much closed, but in fraud cases you will always see they find some way to circumvent it. The internal control framework offers reasonable degree of assurance but not certainty. I think this is more of a risk with sales and purchasing. I recommend changing salesmen and purchasers regularly too prevent them from bonding too much with their suppliers / buyers. However organizations do not like to do this because it hurts their purchasing / sales performance.

13. In your experience what is the effect of familiarization on internal control systems, and how can that effect be minimalized?

It happens. But I would say if it has weak spots you didn't create a proper internal control system. This goes back to the risk assessment, the right risks should be covered with the right controls. What is important for my organization, what is sufficient to cover? What was good internal control 10 years ago is not anymore, it's constantly changing. 10 years ago no one was talking about cyber security and now it is on top 1, 2 and 3 of all organizations.

14. In your experience what is the effect of the gain/loss principal on internal control systems and how can organizations find the quality optimum?

Completely agree with this danger. Again this is about the most important risks and what to cover? On every risk there should be one or more controls both preventive and detective. You should ask yourself do I have double controls. This happens really quickly. When optimizing your control environment you should see your different defense lines, so too what extend does management have assurance on this control? Then there are the 2nd line functions, AO/IC etc. Then there are the internal control teams that check the same things for the third time. I think for a lot of organizations there is room for optimization in this area.

15. In your experience, what is the effect of the financial distress on internal control systems and how can organizations minimize this effect?

Automate what's possible. In small organizations you can rely more on detective controls. And keep working on your soft controls for example culture and behavior.

16. In your experience, are there any other dangers to internal control systems that were not mentioned?

If you take a look at Asia, Africa, and countries like Saudi Arabia. There are different ways of doing business, different norms and values. What we think is abnormal based on our norms and values might be a proper way of doing business in their country. As Dutch organizations do you want to comply with this? Probably not. Within your organization do you have enough attention for internal culture and behavior? For example Japanese organization that operate in Europe are used to install Japanese management. Whereas Dutch organizations in Japan often have an own people first policy. At least installing people that have matching cultures. Have the same norms and values. Other dangers are in soft controls elements, it doesn't matter how well you create an internal control system, if top management sets a bad example, if it is not clear how to follow certain rules, if there's not enough capacity to carry out controls, or if people are too afraid to address one another, your internal control system will not work.

Practical fraud case (optional):

17. Do you have a personal experience with financial statement fraud? If yes, can you describe this case, explain how it came to light, and how according to you it could have been prevented or detected earlier?

No

Interview: C
Date and time of interview: 14 February 2017 14:00-15:00

Interviewee: Audit Partner

Introduction:

1. Are you okay with this conversation being recorded? **Yes**

2. Are there any questions about the research before we start the interview? **No**

3. Can you describe your current employment? **Audit Partner**

4. Can you describe how you come in contact with internal control systems during your work activities?

I carry the main responsibility for some customers. I have different listed customers and national practice customers. But no matter the customer we always check the internal control of the customer, even if only segregation of duties which is important to us. Internal control is a relevant theme, no matter the size of the organization but when the size of the organization increases internal control becomes more important.

Research questions:

Fraud prevention strategies:

5. In your experience what are best practices in preventing financial statement fraud?

This depends on the size and professionality of the organization. In an organization there are different layers of internal review procedures which provide reasonable assurance that no financial statement fraud is taking place. Examples of best practices are code of conduct, whistleblower systems, internal audit function, and audit committee. But again this really depends on the size of the organization. In addition we separate hard controls and soft controls. The examples I just named are hard controls, but soft controls are just as important. Examples are tone at the top, or what kind of example top management sets. It is about the combination between hard and soft controls, one will not do the job.

6. In your experience what are the best controls an organization should have in place for preventing financial statement fraud?

An organization should have at least the following hard controls in place: Segregation of duties and authorization limits. Otherwise it becomes very difficult for us to check. It is important for an organization to know that no commitments are undergoing, without return favor. It is about who is authorized to place an order, what is the maximum amount, what is the margin, how does supplier selection work. It is easier to detect fraud when multiple people are involved in a process, for example who places a purchase order, who receives the goods/service? Who authorizes the invoice? If all these things are with one man or group, fraud becomes hard to detect.

7. What is required for an efficient internal control system?

I think it should be about more effective. It is about applying effective measures to prevent the fraud. Efficiency is about the consideration between costs and gains. An organization can hire 10 extra people, have a perfect internal control system but go bankrupt due to high costs associated. Some companies have small organizations, but even then independent review could take place. Again it depends on size. However it is not always in the means, when I take a look at large listed companies. The board can ask themselves how much risk we are willing to take. Or do we pay the risk premium, the risk premium is in the costs of procedures that cost money but add nothing to the primary process. Examples of these are: internal audit, review of controls, costs of external accountants. This is very much in the risk appetite of the board.

8. What are current fraud prevention strategies?

We just talked about a lot of preventive measures, in the end an organization has to convince me that they have enough measures in place that so that the financial statements do not contain any material misstatements. I think it is a mix of the elements we have named. In larger organizations were IT systems are very rigid, in IT systems there are all kinds of functions which are linked to profiles. When these profiles conflict with one another, this indicates a breach of segregation of duties. That is something you want to know as organization so you can ask, is this risk acceptable or should I address this immediately? However I do not see much organizations analyzing data files, or creating dumps to analyze. We as external accountant do not see every transaction that would require us to sit next to the customer the

entire year. So we select certain control methods to check enough transactions to give us reasonable assurance that the statements are in order.

9. What do internal control systems provide for an organization?

Question not asked.

10. What tools does an organization have to detect fraud?

Question not asked.

Dangers to internal control systems:

11. In your experience what is the effect of management override on internal control systems, and how can that effect be minimalized?

In all audits we see the risk of management override as a presumed risk, which means we assume that it is always present. In 9 out of 10 cases there can be motivation from management to direct results. And we always do verify control measures to mitigate this risk. An example of this is selecting journal entries on the basis of high risk criteria. The entries that meet the criteria are checked integral. In cases of management override there always is a breach of segregation of duties. So an example of what you could do is ask people that worked on financial statements if they were asked to do any bookings without any documentation explaining why.

12. In your experience what is the effect of collusion on internal control systems, and how can that effect be minimalized?

I do not see this very often. Extra question from interviewer: Can you think of a situation in which the risk would be higher? Yes but than you would go into fictional situations. Collusion is very hard to detect. Audit is not specifically aimed at detecting fraud. But we should be very critical when we come across things that could be indicators for fraud. The moment we have even the least suspicion something is wrong, we should open the tool box and perform the right activities. These suspicions can come from meetings with management, but also when doing controls on invoices that seem strange. When this happens you should ask what this invoice is, what is the rationalization behind it, and is the information on the invoice proper. This is a professional critical attitude. In this way we should be very specific and very alert to this threat, but collusion is something you hardly ever see.

13. In your experience what is the effect of familiarization on internal control systems, and how can that effect be minimalized?

If you have good internal control, it stays effective even when people are familiar with the system. A purchaser should never do supplier selection alone and you need to pre determine the selection criteria. If this is the case the only way fraud can happen is through collusion. A lot of lower level (for example administrative) functions are filled by the same person for many years, however this does not mean that the risk of fraud becomes higher if the internal control system is strong enough.

14. In your experience what is the effect of the gain/loss principal on internal control systems and how can organizations find the quality optimum?

This depends on the risk acceptance rate of the board. How much risk are they willing to take? When are they comfortable? When you own the company you have a different perception of risk, then when you are a manager with one shareholder (private or listed company), or when you are a manager with multiple shareholders (listed company). What we as external accountants think comes second, because organizations should be in control themselves. The external accountant is not allowed to give advice to listed companies that is regulated to audit only. When we come across situations in the internal control system when checking the administrative organization of the customer, we provide a report with recommendations and determine the impact on our audit. When the client has questions about how to create a risk control system, we do not provide advice. Instead we refer the client to a specialists advisory. It is important as accountant to not make decisions yourself, do not sit in the chair of the management. Because this creates risks to the accountants independence.

15. What do you advise organizations that are in financial distress in relation to internal control systems?

This is a very difficult question because it really depends on the reason why the organization is in financial distress. I am not an advisor but when I approach it from a control point of view I think it is really important that segregation of duties is accounted for, otherwise it becomes hard to control. And when organizations are in financial distress it becomes even more important for external parties that the financial statements do not contain any material misstatements. It does not help the organization to throw everything overboard and put everything on commerce for example.

16. In your experience, are there any other dangers to internal control systems that were not mentioned?

Do not underestimate the power of culture. When talking about culture it sounds like you are talking about soft controls, but culture is not a control. In the end its important what culture you have as organization. It is very important employees have the right attitude to properly do the controls, and address each other. When thinking about soft controls you often think about tone at the top, or setting the example but it is also about are you asking people things they can actually do? Did you prepare properly? Do you dare to address people when they do not do things right? It is very broad but it is about how your organization work does? And this is a very important aspect to internal control. When the culture is not right, internal control becomes less efficient. You should have enough attention for both hard and soft controls. Otherwise people set their signature where they have to, and for the rest adhere themselves to nothing.

Practical fraud case (optional):

17. Do you have a personal experience with financial statement fraud? If yes, can you describe this case, explain how it came to light, and how according to you it could have been prevented or detected earlier?

No

Interview: D
Date and time of interview: 17 February 2017 09:00-10:00

Interviewee: Audit Manager

Introduction:

1. Are you okay with this conversation being recorded? **Yes**

2. Are there any questions about the research before we start the interview? **No**

3. Can you describe your current employment? **Audit Manager**

4. Can you describe how you come in contact with internal control systems during your work activities?

I do different kinds of audit assignment for different kinds of organizations: construction, education, production, commerce.

Research questions:

Fraud prevention strategies:

5. In your experience what are best practices in preventing financial statement fraud?

Segregation of duties. And critical supervision. However it depends on the size of the organization. I think the supervisory board and internal audit function have important roles.

There should be people in your supervisory board that have knowledge of financial statements, and that dare to ask critical questions and follow up questions.

6. In your experience what are the best controls an organization should have in place for preventing financial statement fraud?

I think the external accountants audit is really important. I think segregation of duties is really important. It should be impossible that one person controls multiple functions. Proper budgeting towards your shareholders is important, because it does not allow for unrealistic expectations. And I think it is important that everyone has enough knowledge of the organization, so that something out of the ordinary is noticed.

7. What is required for an efficient internal control system?

The theory of COSO explains this pretty well. How do you set up your internal control system? What kind of risk analysis do you do? What kind of control activities do you do? The most important part of an efficient control system is I think the monitoring, how do you make sure that your internal control system stays intact? I think the whole picture that is specific for every organization is the most important. The board of directors should have control systems towards their employees, so called checks and balances. On the other side I think internal audit department is important and having a good supervisory board. The supervisory board should be responsible for hiring an external accountant, however in practice you often see that it is management that does this. This creates a conflict of interest because the potential fraudster is hiring the external accountant that could detect his fraud. As external accountant you have meetings with the supervisory board, and the management team. It is important that these parties use your findings.

8. What are current fraud prevention strategies?

Often organizations undertake actions after it goes wrong. I think in a lot of organizations there is a lack of realization that fraud can happen. It is very important to do proper risk analysis. It is possible to put controls on everything but this makes running an organization difficult. Also important how often you update your internal control system for example what was a good internal control system for IT 10 years ago is severely outdated as of now. Another good strategy is the element of surprise, recently external accountants started to do checks that were not pre announced. For example checking the cashbox, or request all bookings from one control.

9. What do internal control systems provide for an organization?

If you do not have an internal control system, you are not in control. When at the start of the year you make a plan for where you are going to go, you need to be able to realize your plan. The most important thing is that you can show a stable growth rate, without internal control this is not possible. It is information you need when for example securing funding from a bank.

10. What tools does an organization have to detect fraud?

Healthy farmers' wit (Dutch saying for logical thinking) is how you often find out. You need to know how an organization works, this way you know when something is out of the ordinary and can do further inquiries. If you do not have enough knowledge of the organization, you could find yourself asking the fraudster for an explanation giving him a chance to rationalize his fraud. Something else is data analysis, by analyzing all available bookings, bookings that are out of the ordinary can be identified. An example of this is when 90% of the bookings run through the sales process, but 10% is booked as memorial booking at the end of the year. This is out of the ordinary and requires further research. A manager might be trying to inflate the organizations revenues. But even this is not a 100% assurance.

Dangers to internal control systems:

11. In your experience what is the effect of management override on internal control systems, and how can that effect be minimalized?

The effect is that you circumvent the entire internal control system. An example of this is when an organization does not want to make a provision, but instead tries to hide the provision under debt. Reasons for this might be the effect it has on law cases that you expect to lose, or employees that you want to fire. An organization could want to fire an X amount of employees per year because of shrinking business, but does not want to show this in the financial statement. This can be prevented by knowing what is happening in the organization.

12. In your experience what is the effect of collusion on internal control systems, and how can that effect be minimalized?

I think this is a very difficult one. When fraudsters are really conspiring it is almost impossible to see for an external accountant. External accountants are victims themselves in these cases. I have not witnessed this myself.

13. In your experience what is the effect of familiarization on internal control systems, and how can that effect be minimalized?

Question not asked

14. In your experience what is the effect of the gain/loss principal on internal control systems and how can organizations find the quality optimum?

I think it is all about doing a really good risk analysis, and then asking what you are going to cover and what not. I think most organization do this pretty well for the regular processes. Examples of flaws that organizations fail to cover are often in payment, for example that after a payment has been authorized by a manager the payment order can still be changed.

An example of what you see is that an invoice comes in, this must be made payable so a payment document is generated, this document is often an xml file that can be changed this is saved in an unsafe place or the file is authorized by management but is changed in the financial system after the authorization has taken place. One could for example change the suppliers' bank account to the fraudsters' bank account. Ideally the file would be read through telebanking, authorized and unchangeable after that. This is an example of the entire process being controlled except of the last step.

15. What do you advise organizations that are in financial distress in relation to internal control systems?

Financial distress increases the chance of financial statement fraud. In cases of financial distress I think the supervisory board is very important. When organizations are in financial distress the management team should report a plan for coming out of the crisis. The board should supervise the attainability and realism of this plan.

16. In your experience, are there any other dangers to internal control systems that were not mentioned?

The difference in knowledge between shareholders and the management team. The less knowledge the shareholders have the larger the risk of financial statement fraud. Low knowledge of shareholders is an indicator for a weak internal control system. Appointing a supervisory board should decrease the gap in knowledge.

Practical fraud case (optional):

17. Do you have a personal experience with financial statement fraud? If yes, can you describe this case, explain how it came to light, and how according to you it could have been prevented or detected earlier?

I have a private matter. We had a management bureau that did the administration but this was expensive. One person offered to do this voluntarily, only expenses for an accounting system were declared. He did this for two years. After which everyone received an email saying the treasurer was caught transferring money to his own account. The fraud was detected because the treasurer missed meetings of the board, the board demanded the treasurer would attend board meetings or replace him. The treasurer was fired, when the board received the administration they compared the bank balance to what was expected from the financial statements. The financial statement he filed at the end of the year did not show any misstatements. The treasurer was checked by a cash commission that compared bank notes to financial statements. However the bank notes were copies forged by the treasurer, had the fraudster not been discovered he could have kept doing this until cash ran out. A four eyes principle on bank payments could have prevented this fraud.

Interview: E
Date and time of interview: Friday 17 February 10:00-11:00

Interviewee: Audit Manager

Introduction:

1. Are you okay with this conversation being recorded? **Yes**
2. Are there any questions about the research before we start the interview? **No**
3. Can you describe your current employment? **Audit Senior Manager**
4. Can you describe how you come in contact with internal control systems during your work activities?

I am responsible for the team that carries out the audit at the customer, while also being the customer's contact for questions. In the planning phase we perform the risk assessment, and determine our audit plan how to deal with them in the audit. During the control testing face we have to decide if we will test existing internal control measures. And when we decide to lean on existing measures, we have to see which internal control measures the customer put in place, whether they exist, and if we can test them. Based on that we can decide on the testing sample for substantive procedures. In addition to this we have to document how the entity level controls are set up. Entity level controls are on organization levels, examples of this are risk management, control environment, monitoring: for example which risks has the organization identified, which measures have they taken on identified risks. How do they monitor?

Research questions:

Fraud prevention strategies:

5. In your experience what are best practices in preventing financial statement fraud?

Set good internal control measures. Ensure adequate segregation of duties between different steps in the processes. Proper tone at the top from management: How do you handle this, what is your own policy, how do you supervise it? On one hand it is in hard controls, on the other hand soft controls are also important. Culture, behavior, transparence that type of business.

6. In your experience what are the best controls an organization should have in place for preventing financial statement fraud?

Segregation of duties between different functions in the process, it is really important that the steps: entering into a transaction, authorizing a transaction and recording the transaction

are done by different people. No matter what process you focus on, in the end it should always be about having different people perform different tasks in the process. I also think it is important having someone check his colleagues work. That would be the most ideal. For example the price list for sales: One person creates the price list, one person enters it into the system, and one person checks whether the first two have done it right. This way you check whether the internal control measures you have set up, are actually performed in the right way. It is important that this is visible for the auditor, otherwise the auditor cannot rely on it for the audit.

7. What is required for an efficient internal control system?

It is important that on the right controls have been implemented to provide assurance on the critical steps in the process. For example it cannot be that in the payment process one employee is doing the placement of the order, the payment and the receipt of goods. Sometimes in very small organizations this will be the case, but then it is a decision of management, but it is not something you want in an ideal process.

8. What are current fraud prevention strategies?

It depends on the organization. Internal control measures are important. A new development is that more organizations focus on soft controls. It is very important that employees are aware of the purpose for internal controls. In our own audits I see that auditors are more using substantive testing (including data analysis) and less testing of effectiveness of internal control measures. Where necessary we see the entire population. Another development is the recommendation for large organizations (especially listed entities) to have their own internal audit departments.

9. What do internal control systems provide for an organization?

These provide Assurance, confidence about what is coming in and what is going out (especially money coming in and going out).

10. What tools does an organization have to detect fraud?

To detect financial statement fraud organizations can perform their own assessment regarding their financial statements where are these numbers in the financial statements coming from, are they right? Did we challenge ourselves as company enough? Another option might be to hire an external consultant, sometimes organizations hire an external company to perform specific procedures (for example detecting if a company have paid a same invoice twice).

Dangers to internal control systems:

11. In your experience what is the effect of management override on internal control systems, and how can that effect be minimalized?

The effect is that internal controls are either way not used, or that after controls have taken place a manager simply tells an employee to do it. This can be prevented by being critical towards questions asked by management as organization. Ask yourself does this make sense to me? Is the manager right and is this allowed by rules and regulation? This is what I call a professional critical attitude.

12. In your experience what is the effect of collusion on internal control systems, and how can that effect be minimalized?

The effect would be that the internal control system would fail. Internal control measures would cease to be effective. An organization can prevent this by switching employee's roles and functions. An example of this is the steps from the sales process, having employee A perform a different step in the process every x period.

13. In your experience what is the effect of familiarization on internal control systems, and how can that effect be minimalized?

The effect would be that the internal control measure put in place to prevent/detect something would fail to work as an employee would find a way to circumvent the control. Also here I think switching employees is a good option. Do not let your employees do the same things for too long. Another option would be to have someone external check whether your control is effective, or if there are any flaws. You could ask your auditor to do this, hire an external consultant or start an internal audit department.

14. In your experience what is the effect of the gain/loss principal on internal control systems and how can organizations find the quality optimum?

The effect is that you see organizations ask themselves, what additional gains can I get from this, do I think this provides me with additional assurance and does this outweigh the costs? But I think it is important to see the total picture, for example having an effective internal control system means the accountant has to do less work which in turn means less costs.

15. What do you advise organizations that are in financial distress in relation to internal control systems?

When management fraud happens management will more likely try to influence judgmental posts like provisions? The problem with this is that there are only a few employees in the organization that have enough knowledge on this subject. The question is how critical these employees will be when someone tries to convince them with a very good story that a certain provision is unnecessary /should be higher. Auditors have to audit the assessment of management and if something does not comply with the rules, when something is wrong it is wrong the client should change it in the financial statements. Often these kinds of accounts are estimates, and the question is how well can management explain their estimate? An auditor has to challenging the client when auditing accounts like provisions.

16. In your experience, are there any other dangers to internal control systems that were not mentioned?

Apart from hard controls it is also very much about the experience of employees and their drive to comply with rules, and follow procedures properly. Because when you have internal control measures that are always overridden, and never complied with without anyone caring about it they are ineffective. This culture does not provide any incentive for the employee to actually comply with the internal control system. I think this is really important, some people claim the soft controls are more important than the hard controls. Because when everyone knows why they do it and how, you do not need any hard controls. Another danger to internal control system is the exception to the rule, you can have all kinds of procedures and rules but how do you handle business that falls just outside of those rules and procedures. Do you ignore them or do you have separate controls for that? Does your employee follow the procedure, and what seems logical to him or does he think this is not on my list so I do not need to do anything with this.

Practical fraud case (optional):

17. Do you have a personal experience with financial statement fraud? If yes, can you describe this case, explain how it came to light, and how according to you it could have been prevented or detected earlier?

I have no experience with financial statement fraud however I have seen one case in which someone ordering a product used incorrect client information. This can be prevented by calling the customer on the office number, checking the client with the chamber of commerce, request

for prepayment of the invoice. Requesting prepayment of the invoice is probably the best preventive method in order to make sure the receipt of cash.

Interview: G
Date and time of interview: 1 March 2017 15:00-16:00

Interviewee: Forensics Manager

Introduction:

1. Are you okay with this conversation being recorded? **Yes**

2. Are there any questions about the research before we start the interview? **No**

3. Can you describe your current employment? **Senior Manager Forensics**

4. Can you describe how you come in contact with internal control systems during your work activities?

I have been working for this organization for 10 years. The first five years I worked in the audit department and after that I changed to forensics. Here in the beginning I did traditional fraud research, but because of my audit background I supported audit as well in fraud related subjects. I also worked on offenses of laws and regulations. Examples of this are corruption investigations, tax evasions and related offenses.

Research questions:

Fraud prevention strategies:

5. In your experience what are best practices in preventing financial statement fraud?

Good culture, and awareness I think those are very important. When reviewing an organization you can check for tone at the top, proper corporate governance, communication of corporate governance about subjects like fraud and integrity. How clear is the code of conduct? Are there periodical trainings with the goal of keeping awareness high? Do people dare to address each other on mistakes?

6. In your experience what are the best controls an organization should have in place for preventing financial statement fraud?

Four eyes principle and segregation of duties are very important. There can be no functions or authorizations that are contradictory. I think also training of your employees, so they know what they are doing and why. And who is authorized to do what? Training about the systems, so they can see when something someone else does is out of the ordinary. Familiarity with the systems. And last I think your bonus policy is very important, but this is more towards soft controls. When you have very strict targets to bonuses, this stimulates people to commit fraud.

7. What is required for an efficient internal control system?

I think I mentioned the most important things in the last two questions.

8. What are current fraud prevention strategies?

I see cyber fraud is coming up. Technology is on the rise and everything is done digitally. Organizations are not fully aware of the risk that this brings, and are unaware how to control this risk. Controlling this risk is partly in IT and partly in awareness of employees. Employees have to know what to do when phoned by someone claiming to be the CEO and requiring them to do a payment.

9. What do internal control systems provide for an organization?

Internal control contributes to achieving the strategic goals set by the organization. It makes sure that no things happen that are not supposed to happen and that processes go the way you want them to go.

10. What tools does an organization have to detect fraud?

A good analysis of your financials. Proper authorization of invoices and outgoing cash flows. Your payment organization has to be closed entirely. In addition to this you can do data analysis that identify deviations, this does not happen a lot. And good monitoring, audit, compliance audit, internal audit.

Dangers to internal control systems:

11. In your experience what is the effect of management override on internal control systems, and how can that effect be minimalized?

It happens. The effect depends on the structure, in a DGA structure (Director also large shareholder) management override is really hard to prevent. The external accountant would be the one to detect this fraud. The larger organizations become generally the better the payment structure is realized, even in organizations with a DGA structure. In other cases the segregation of duties is very important. And good reviews on journals that have an estimation element.

12. In your experience what is the effect of collusion on internal control systems, and how can that effect be minimalized?

This happens and its effect is a lot more difficult to minimalize. I think the most important controls are culture and awareness. Employees should be aware not to share their passwords, this awareness can be increased by trainings.

13. In your experience what is the effect of familiarization on internal control systems, and how can that effect be minimalized?

What we talked about before you take preventive measures, but we also talked about how to detect a fraud. As an organization it is very important to have a good balance between both. So you have to test if your controls are working, if your employees are actually doing them, and last you have to see if there are no irregularities in your data.

14. In your experience what is the effect of the gain/loss principal on internal control systems and how can organizations find the quality optimum?

I think this is definitely a consideration organizations have to make. Because you can close everything, but this would cost too much or your organization would be unable to work. When talking about corruption risk an option is to only do business in the Netherlands and stand behind the check-out counter yourself so that you are sure no fraud is taking place, but this way your organization will not grow. So there is a continuant estimate of costs and risks, what I think is very personal for organizations. Insight in the risks the organizations faces is very important. Then an organization has to decide its risk appetite, which is how much risk is it prepared to take. And those two together decide how much an organization has to invest in internal control. One organization might be more risk averse then the other.

15. What do you advise organizations that are in financial distress in relation to internal control systems?

I understand that organizations that are in financial distress have a higher fraud risk, to meet your bank covenants or to keep your shareholders satisfied. But I do not think it is logical to assume that organizations that are in financial distress generally have less resources to spend on internal control. I think that these can be seen as fully separate, because you can have an organization that did well with a good internal control system that suddenly takes a turn for the worse, but your internal control system would still be sufficient. You can also have an organization that does really well but grows faster than its internal control can follow (this is what happened at LCI). So I do not necessarily see a correlation between organizations that are in financial distress and a weak internal control system.

16. In your experience, are there any other dangers to internal control systems that were not mentioned?

We talked about the gain/loss principal, I think that when you spend too much on internal control you stimulate people to do processes differently. Because it is no longer workable. For example if employees have to do many registrations or proceedings before they can actually work

and they see a way to prevent having to do this many registrations and proceedings they are more likely to do this when the process is not workable. Or when you say I have to fill in so much check and balances, I will do it some other way.

Practical fraud case (optional):

17. Do you have a personal experience with financial statement fraud? If yes, can you describe this case, explain how it came to light, and how according to you it could have been prevented or detected earlier?

The board of an organization got a message from a supplier that it was deliberately being kept out of tenders by the organizations purchasers because other suppliers bribed their purchasers. The board has to act on this because it is proof of a fraud going on, and hired an external agency to investigate the purchasers. The purchasers had worked for the organization for years and were trusted thus the board hoped the accusations proved to be false but wanted to do independent research. The research was done by investigating e-mail traffic and holding interviews with several people. The result of the research proved conflict of interest between suppliers and purchasers. An example is the purchasers were taken on a fully compensated trip to the supplier's factory in Italy. With half a day factory visit, and three days of golfing so to speak. And more trips like this one. The purchasers claimed to be objective, and claimed to have chosen the best supplier for the contract. However were fired nonetheless. How could this have been prevented? In this case you saw two purchasers that were authorized to do a lot on own accord. Of course they had to write a tendering contract which explained the criteria, however they were allowed to choose other suppliers based on qualitative measures. Also there was a supervisor that gave the purchasers too much freedom. The organization did have guidelines on what to accept and what not, but the rules were interpreted differently. For example one of the employees claimed that the trip was not done during work time and therefore the trip is not work related. Or the supplier is also my private friend and therefore he takes me golfing and pays for me. However even when being friends, it is still not allowed to have a supplier pay trips for you without announcing it to management. I think this was difficult to prevent, but what they do now is pay much more attention to awareness. So focus on what can you accept, what can you not accept? When do you create a conflict of interest? Concluding these people have been fired and this case has been spread in the company to set proper tone at the top.