HAAGA-HELIA
University of Applied Sciences

Financial Fraud - Importance of an Internal Control System

Jenna Saarni

Bachelor's Thesis

Degree programme in International Business

2012

HAAGA-HELIA
University of Applied Sciences

Abstract

5 Nov 2012

International Business

Author Jenna Saarni	**Group or year of entry** GloB09S
Title of report Financial Fraud - Importance of an Internal Control System	**Number of pages and appendices** 65 + 6
Teacher(s) or supervisor(s) Jari Luomakoski, Jaana Melamies, Elizabeth SanMiguel, Teppo Varttala	

This thesis tackles the problem of financial fraud, and the goal of the research has been to investigate the importance and the efficiency of internal control systems. The precise research problem is; how to prevent accountants and managers from conducting financial fraud – importance of having an internal control system? The thesis has been commissioned by HAAGA-HELIA University of Applied Sciences, which expects to receive valuable research concerning ethics in financial accounting.

To approach the problem, first some theory behind fraud, risk management and internal control will be looked at. The two of the most famous financial fraud cases, Enron and the Lehman Brothers, will be shortly presented. These, and an overview of a research on fraudulent financial reporting in U.S. public companies, will give the reader an insight of the seriousness of the topic.

The research has been focused on consultants, as experts of the topic, representing the Big Four auditing companies. In addition to these, a recent fraud case in Company X has been examined. The data collection has been conducted with the use of a Webropol survey and interviews. The research process has taken place during late spring and early autumn 2012.

The collected data has been analysed with comparison to the theory framework. The COSO ERM and the COSO cube -model are the main measurement tools used in the analysis. The research and findings were completed in October 2012. As the main findings, the paper presents that an internal control system should be a part of every organisation's risk management, however the depth of the system should be in proportion with the size of the company and the corporate culture. Based on the COSO cube –model and the presented findings, the essential consideration for companies should be in creating functioning components of the internal environment, information and communication flow, as well as event identification.

Keywords
Internal control, financial fraud, unethical accounting, COSO, enterprise risk management

Table of contents

1 Introduction

As long as humans have existed, fraud and betrayal have as well. For some reason, it seems also as though greed for money and success are part of human nature. During the past years numerous amounts of corporate accounting scandals have been in the headlines, probably the most known ones have been the Enron case in 2001 and in 2008 the Lehman Brothers case.

Enron and their accounting firm Arthur Anderson systematically produced fraudulent financial reports and engaged in unethical accounting by misrepresenting earnings and hiding liabilities and debts (Roger 2010). When the depth of the deception came out to the public, investors and creditors retreated, forcing the company into bankruptcy in December 2001. The scandal that happened with Lehman Brothers was similar. Lehman Brothers was the fourth largest investment bank in the US, and the bankruptcy it had to file was the largest ever made in US history. The company regularly used accounting gimmicks at the end of each quarter to make its finances appear less shaky than they really were. After the fall of Lehman Brothers, other banks followed and this is believed to be the beginning of the 2008 starting global financial crisis. (Bloomberg BusinessWeek 2009.)

One interesting fact is that most of these big companies gotten caught of fraud in financial reports have been audited by the Big Four auditing firms: PricewaterhouseCoopers, KPMG, Ernst & Young and Deloitte Touche Tohmatsu (Wikipedia 2012). This rises up questions on how it has been possible to scam the ones who should be there to reassure the reliability of the records. Or could there be something behind the scenes? Even though large companies are the ones ending up in the news, small firms experience fraud and unethical behaviour evenly as much.

Implementing an internal control system is believed to be one of the fraud prevention strategies. Many theory books as well write about the fraud triangle - motive, opportunity and rationalisation – representing the three corners (Harrison, Horngern,

Thomas & Suwardy 2011, 236). If all of three corners of the triangle exist a high possibility for a person to commit fraud exists.

The thesis will take a look at internal control procedures, in theory and in practice. In order to get a better picture on the topic, the thesis will begin with fraudulent accounting cases and continue with theory on internal control with different concepts and models. Research on what now is happening in consulting companies will be made by a survey and interviews. The final goal is to find out whether implementing an internal control system can actually prevent fraud.

1.1 Thesis topic

As the name of the report, Fraudulent Accounting - Importance of an Internal Control System, suggests the thesis will be based on ethical issues related to accounting, which include the compliance with international accounting standards, local laws and regulations, and the importance of having an internal control system. Fraudulent accounting and internal control fall under the phenomenon of risk and management accounting, which should nowadays be a part of all enterprises. Effective risk management includes risk assessment, risk evaluation, risk treatment, and risk reporting (Collier, Berry & Burke 2007, 10). The thesis will take a look at the importance of internal control and the different possibilities of how companies are able to "cook the books" and in which way this kind of behavior can be prevented.

The goal is to find out how accountants and managers should be controlled and/or motivated to conduct ethical behaviour in financial accounting, so that companies would produce truthful and reliable financial records. The interest is also in why does fraud happen and how can it be prevented already in the very initial stages.

1.2 Research problem and investigative questions

The research problem for the thesis is:
How to prevent accountants and managers from conducting financial fraud – importance of having an internal control system?

The investigative questions are (hereinafter IQ's):

- IQ1: What are managers' views on internal control generally and in their company? Example of real practice: current internal control system.
- IQ2: How efficiently does an internal control system prevent fraud?
- IQ3: How to prevent fraud in the very initial stages? And what are the development ideas and suggestions to improve internal control?

In addition to researching the investigative questions, the theoretical background will include research on challenges and problems concerning ethics in accounting and internal control, as well as "failure points" on what have happened in the past by presenting examples of Lehman Brothers and Enron. By doing the background and the empirical research, the final results of the thesis should represent a thorough answer for the research problem.

The overlay matrix includes all the essential information on what the thesis and research at hand includes (attachment 1). Starting from the research problem, and then breaking it down to the investigative questions, the overlay matrix presents the theoretical framework, measurement questions used and finally the results. Each of the mentioned applied separately for each investigative question.

1.3 Demarcation

This is a business management problem in the field of finance, and more specifically in accounting and consultation companies. The focus is on daily work, related to control and motivation from the management to the employees. The focus is between three parties: manager, accountant and outside auditor, but this thesis will mainly focus on the management's point of view. The aspect of control will be discussed from a company's internal aspect, and there will be no focus on external control presented.

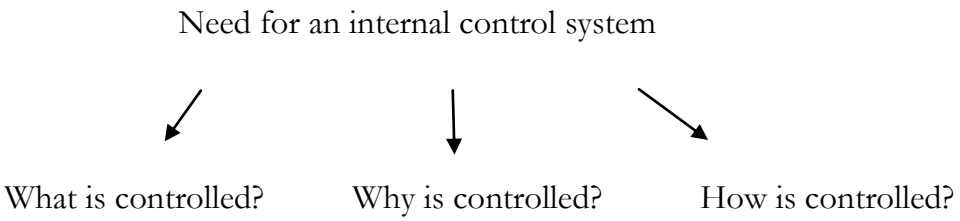

Figure 1. Demarcation questions

The three questions presented above will be the core for the thesis and the answers to these questions will be deeply discussed (figure 1). Similarly questions related to fraud will need to be answered. Conceptualizing the research problem to:

- How to prevent accountants and managers from conducting unethical behavior in financial accounting – importance of having an internal control system?
  And:
- What recommendations can be given based on the research findings?

1.4 Key concepts

This chapter presents the definitions of the key concepts used throughout the thesis. The concepts will be discussed in more detail in chapter 2, the theory framework.

- **Fraud:** Misrepresentation of facts, purpose of persuading another party to act in a way that causes injury or damage to that party (Harrison et al. 2011, 233).
- **Internal Control:** A system of procedures implemented by company management. It is designed to follow objectives as: safeguard assets, encourage employees to follow company policy, promote operational efficiency, ensure accurate, reliable accounting records and comply with legal requirements. (Harrison et al. 2011, 237.)
- **Risk management:** The process of understanding and managing the risks that the organisation is inevitably subject to in attempting to achieve its corporate objectives (Collier et al. 2007, 10).

- **The Big Four:** Refers to the four currently biggest auditing and consultancy companies: KPMG, Ernst & Young, Deloitte Touche Tohmatsu and PwC (PricewaterhouseCoopers) (Financial Times Lexicon 2012).

1.5 Commissioning company

The thesis has been commissioned by HAAGA-HELIA University of Applied Sciences. A part of the Degree Programme in International Business is to educate and guide students to become ethical thinkers, who act in a social responsible way (HAAGA-HELIA 2012a). The ethical issues related to finance and financial accounting discussed so far during the actual courses, are quite limited. Therefore, the thesis and research presented here bring added value to the degree program and provide new insight to fellow students.

HAAGA-HELIA University of Applied Sciences is part of the Finnish public educational system, which is run privately but steered and co-funded by the Finnish Ministry of Education and Culture. The university has around 10 500 students and 700 employees, who base their activities on highly advanced national and international expertise. The school provides education on business, hotel, restaurant and tourism management, information technology, journalism, management assistant training, sports management and vocational teacher education. (HAAGA-HELIA 2012b.) The author and researcher of this thesis has studied international business and specialised in finance.

By commissioning this thesis, HAAGA-HELIA expects the research to provide valuable findings on ethical issues related to finance in an international context. By linking theoretical concepts to actual real life practices, the topic of financial fraud will become more explicit for future students and graduates. Therefore provide added value for the degree program as well as future students.

2 Theory framework

First as theoretical background on the topic, the basic concepts related to fraudulent accounting and the theory around existing internal control systems needs to be explained. This part of the report will mainly answer to two questions:

- 1: What are the challenges and problems concerning ethics in accounting and internal control?
- 2: What has happened in the past – "failure points" of case examples: Lehman Brothers and Enron.

2.1 Fraud

Fraud is one of the top concerns for corporate executives. During the recent years many organizations have faced corporate scandals due to fraud, making the executives face the consequences of large fines and prison time (Ernst & Young 2009). The term, fraud, can be defined as the misrepresentation of facts, purpose of persuading another party to act in a way that causes injury or damage to that party (Harrison et al. 2011, 233). A model, the Fraud Triangle, created by criminologist Donald R. Cressey, represents the three factors that push an ordinary person to commit fraud (figure 2).

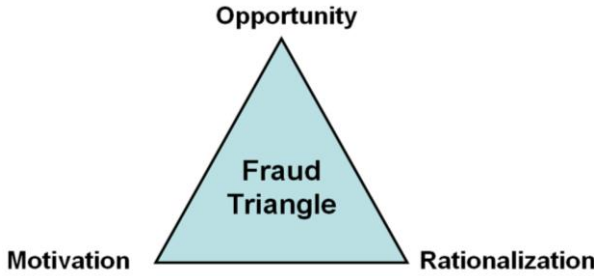

Figure 2. The Fraud Triangle (UCMerced 2012)

If a person has all the three ingredients, motivation, opportunity and rationalization, a high possibility to commit fraud exists (Harrison et al. 2011, 234).

From these three factors, motivation and opportunity are something the organisation can have an effect on. These two are directly influenced by the corporate environment and further more by management. The opportunity can arise by the lack of control and security within the company. The motivation, or pressure (as referred by Ernst & Young), can be created by demands of higher earnings, or it can also arise from the top of the company. A tone that places an impropriate emphasis on financial results or stock price may send the message that cutting corners is acceptable. (Ernst & Young 2009, 1.) Rationalisation is more of a psychological factor, which arises from within the individual person. By rationalising the fraudulent behaviour, the person committing the fraud assures him or herself that it is acceptable to be doing so. (Harrison et al. 2011, 234.) To give an example, a person could rationalise stealing money, as "I have always worked so hard, therefore I deserve it", this way a person makes the act feel as if it was justified.

The common types of corporate fraud are misappropriation of assets, fraudulent financial reporting and corruption. From these the first one mentioned is the most common one. According to the 2008 ACFE Report to the Nation on Occupational Fraud & Abuse, asset misappropriation accounted for 88.7% of the incidents reported. Corruption came second at 27.4%. The concept of corruption includes conflicts of interest, bribery and extortion. In the study fraudulent financial reporting accounted for 10.3% of incidents, which was the least frequent form of occupational fraud. (Ernst & Young 2009, 1.)

2.2 Financial fraud

According to Harrison et al. (2011, 235), the two most common types of fraud impacting financial statements are:

- 1. Misappropriation of assets: employees steeling money and covering it up by making wrong entries to bookkeeping.
- 2. Fraudulent financial reporting: managers making false and misleading entries to the financial statements, making the company to appear better than in reality.

Even though fraudulent financial reporting seems to be the least frequent form of fraud, it is by far the most expensive, in terms of both money and long-term damage. According to the same ACFE report mentioned before, the median loss of a fraudulent statement incident was $2 million, compared with $375,000 for corruption and $150,000 for asset misappropriation. In addition to the monetary losses, the company loses its investor confidents, its reputation is damaged and on top of all high fines and criminal actions are at hand. (Ernst & Young 2009, 2.)

The Association of Certified Fraud Examiners has developed a list of common accounting fraud schemes and associated red flags, on which managers should be aware of. These schemes and related red flags mostly happen with overstating revenues, understating expenses or improper asset valuation. The following paragraphs will describe these and the related red flags in more detail.

Overstating revenues or incorrectly recognizing revenues are one of the most common types of fraud on financial statements. The schemes include: recording gross revenue, instead of net; recording revenues of other companies when acting as a "middleman"; recording sales that have not happened; recording future sales in the current period and; recording sales of products that are out on consignment. The red flags in these kinds of situations are: increased revenues, without a corresponding increase in cash flow; unusual or highly complex transactions, especially ones closed near the end of a financial period; in receivables the unusual expansion of days' sales; or high revenue growth when competitors are experiencing weak sales. (Ernst & Young 2009, 2.)

One other common type of financial statement fraud is **understating expenses**. This leads to higher operating income and overall net income. The schemes in these kinds of cases include: reporting cost of goods sold as a non-operating expense so it does not negatively affect gross margin; capitalizing operating expenses, so recording them as assets instead of as expenses; and some expenses are left out recording, or they are recorded in the wrong period. Red flags related to these can be: unusual increase in income, unexpected increase in assets, or allowances for sales returns, warranty claims,

and others that are shrinking in percentage terms or are otherwise out of line with the companies from the same industry. (Ernst & Young 2009, 3.)

Improper asset valuation is also a type of fraud used. The schemes used are manipulating reserves, changing the useful lives of assets, not making a write down when needed, and manipulating the fair value of assets. The red flags related to these include: repeating negative cash flows, but reporting of earnings; noticeable decrease in customer demand and increasing business failure in the industry or the economy; or estimates on assets, liabilities, revenues and expenses are based on subjective subjects and high uncertainties.

Some other schemes related to fraudulent financial reporting can also relate to: so called smoothing of revenues, so overestimating liabilities during "good" periods, and storing away funds for future use; reporting information improperly, especially when it comes to issues related to "party" –transactions and loans to management; or executing highly complex transactions. (Ernst & Young 2009, 4.)

According to the same ACFE's 2008 report, as mentioned before, 66% of occupational fraud was detected by tips or by accident. The survey revealed that tips were the most frequently reported source of initial detection (46%), followed by accident (20%). 19% of fraud was uncovered by internal audit and 23% was uncovered by internal controls. Even though the advancements in technology and the highly regulated climate, it seems that the leading source of fraud detection is still by tip or by accident. (Ernst & Young 2009, 4.)

2.3 Highlights in financial reports

This chapter will visualise the financial reports and pinpoint the specific lines were the most common types of fraud on financial statements have occurred. To take an example, the chapter will examine reports presented by Lehman Brothers Holdings Inc. delivered to the US Securities and Exchange Commission the same year the company filed for bankruptcy. First to observe are some examples from the Lehman Brothers quarterly income statement 2008, before the bankruptcy (figure 3).

LEHMAN BROTHERS HOLDINGS INC.
Consolidated Statement of Income
(Unaudited)

In millions, except per share data	Three Months Ended May 31, 2008	2007	Six Months Ended May 31, 2008	2007
Revenues				
Principal transactions	$(3,442)	$ 2,889	$(2,670)	$ 5,810
Investment banking	858	1,150	1,725	2,000
Commissions	639	568	1,297	1,108
Interest and dividends	7,771	10,558	17,405	19,647
Asset management and other	414	414	853	809
Total revenues	6,240	15,579	18,610	29,374
Interest expense	6,908	10,067	15,771	18,815
Net revenues	(668)	5,512	2,839	10,559
Non-Interest Expenses				
Compensation and benefits	2,325	2,718	4,166	5,206
Technology and communications	309	287	612	553
Brokerage, clearance and distribution fees	252	201	504	395
Occupancy	188	152	373	298
Professional fees	100	120	198	218
Business development	87	100	175	184
Other	158	55	235	127
Total non-personnel expenses	1,094	915	2,097	1,775
Total non-interest expenses	3,419	3,633	6,263	6,981
Income before taxes	(4,087)	1,879	(3,424)	3,578
Provision for income taxes	(1,313)	606	(1,139)	1,159
Net income	$(2,774)	$ 1,273	$(2,285)	$ 2,419
Net income applicable to common stock	$(2,873)	$ 1,256	$(2,408)	$ 2,385
Earnings per common share:				
Basic	$ (5.14)	$ 2.33	$ (4.33)	$ 4.42
Diluted	$ (5.14)	$ 2.21	$ (4.33)	$ 4.17
Dividends paid per common share	$ 0.17	$ 0.15	$ 0.34	$ 0.30

See Notes to Consolidated Financial Statements.

Figure 3. Lehman Brothers consolidated income statement (United States Securities and Exchange Commission 2008, 4)

As discussed in the previous chapter, overstating revenues or incorrectly recognizing revenues are one of the most common types of fraud affecting financial statements. This can be seen in the income statement under different headings, as highlighted in figure 3. As you will read in the upcoming chapter (2.4.2), one of the gimmicks used by Lehman Brothers was to incorrectly recognize revenues. Understating expenses can also be used in making the operating income and overall net income seem higher. In the Notes to the statements, Lehman Brothers describes their revenue recognition policies, under Principal transactions, as follows:

> Realized and unrealized gains or losses from Financial instruments and other inventory positions owned and Financial instruments and other inventory positions sold but not yet purchased, as well as the gains or losses from certain short- and long-term borrowing obligations, principally certain hybrid financial instruments, and certain deposit liabilities at banks that the Company measures at fair value are reflected in Principal transactions in the Consolidated Statement of Income. (United States Securities and Exchange Commission 2008, 11.)

According to this, it can be interpreted that many complicated financial instruments and transactions have been used by the company, and therefore, in this case, it has been able to disguise something that should have been reported as borrowings, under revenues.

Similarly, the balance sheet can be presented in a fraudulent manner. As discussed in the previous chapter, improper asset valuation is also a type of fraud companies have used. The possible fraudulent procedures can include manipulating reserves, changing the useful lives of assets, not reporting down when needed, and manipulating the fair value of assets. Figure 4 presents some of these points highlighted. To give an example, Lehman Brothers' Notes on how the long-lived assets have been valued are as follows:

> Property, equipment and leasehold improvements are recorded at historical cost, net of accumulated depreciation and amortization. Depreciation is recognized using the straight-line method over the estimated useful lives of the assets. Buildings are depreciated up to a maximum of 40 years. Leasehold improvements are amortized over the lesser of their useful lives or the terms of the underlying leases, which range up to 30 years. Equipment, furniture and fixtures are depreciated over periods of up to 10 years. Internal-use software that qualifies for capitalization under AICPA Statement of Position 98-1, Accounting for the Costs of Computer Software Developed or Obtained for Internal Use, is capitalized and subsequently amortized over the estimated useful life of the software, generally three years, with a maximum of seven years. The Company reviews long-lived assets for impairment periodically and whenever events or changes in circumstances indicate the carrying amounts of the assets may be impaired. If the expected future undiscounted cash flows are less than the carrying amount of the asset, an impairment loss is recognized to the extent the carrying value of the asset exceeds its fair value. (United States Securities and Exchange Commission 2008, 16.)

LEHMAN BROTHERS HOLDINGS INC.
Consolidated Statement of Financial Condition
(Unaudited)

In millions	At May 31, 2008	At Nov 30, 2007
Assets		
Cash and cash equivalents	$ 6,513	$ 7,286
Cash and securities segregated and on deposit for regulatory and other purposes	13,031	12,743
Financial instruments and other inventory positions owned (includes $43,031 in 2008 and $63,499 in 2007 pledged as collateral)	269,409	313,129
Collateralized agreements:		
Securities purchased under agreements to resell	169,684	162,635
Securities borrowed	124,842	138,599
Receivables:		
Brokers, dealers and clearing organizations	16,701	11,005
Customers	20,784	29,622
Others	4,236	2,650
Property, equipment and leasehold improvements (net of accumulated depreciation and amortization of $2,697 in 2008 and $2,438 in 2007)	4,278	3,861
Other assets	5,853	5,406
Identifiable intangible assets and goodwill (net of accumulated amortization of $361 in 2008 and $340 in 2007)	4,101	4,127
Total assets	$639,432	$691,063

See Notes to Consolidated Financial Statements.

Figure 4. Lehman Brothers consolidated Assets, balance sheet (United States Securities and Exchange Commission 2008, 5)

Even though in Lehman's case, there hadn't been any improper asset valuation, the balance sheet and the Notes present an example of where fraudulent reporting could take place. As the Notes explain, the property, equipment and leasehold improvements are valued at historical cost, which for example could mean that the inflation or other economic factors affecting the values have not been taken into consideration. As a more detailed example, it mentions that buildings are depreciated up to a maximum of 40 years. One could imagine a building's value could easily change in such a long period. Nevertheless, the company provided financial statements, which were produced fraudulently but was not gotten caught, even by the auditors. As a conclusion for this chapter, one can say that a complex business provides complex financial statements, therefore the ones analysing the reports explicitly need to have the detailed know-how and education for it.

2.4 Company cases on fraudulent accounting

To better understand the seriousness and the depth of the damage of fraudulent financial accounting, this chapter will take a short look at what has happened in the past. As two the most famous cases have been with Enron and the Lehman Brothers, it is natural to look in to these in more detail. However, one must bear in mind that smaller companies face same problems, even though the damages are not in such a big scale. As a conclusion for this chapter, we will take a look at a research, done by COSO, on fraudulent financial reporting 1998-2007: An Analysis of U.S. Public Companies.

2.4.1 Enron

Enron was founded in 1985 through a merger of two natural gas pipeline companies, Houston Natural Gas and Internorth. The company owned around 59 500 km of pipelines transporting natural gas between producers and utilities. To achieve further growth Enron engaged in a diversification strategy. By 2001 the company owned and operated internationally gas pipelines, electricity plants, pulp and paper plants, broadband assets and water plants. In addition the company traded in financial markets

with the same products and services. As the operations of Enron expanded, so did their performance in the stock market. (Palepu & Healy 2003, 3-5.)

Through years, as Enron's operations grew into different levels, its business model turned more complex. This lead to difficulties with the financial reporting, making the company face the limits of accounting. Two issues where specifically problematic. First of all, the trading side of the business involved complex long-term contracts. Enron used an approach called mark-to-market accounting to recognise income. This meant that the management was making forecasts of energy prices and interest rates well into the future, whereas current accounting rules require the use of present value calculations. Secondly, Enron heavily relied on structured finance transactions, which involved setting up special purpose entities. These transactions included shared cash flows and risks with outside investors and lenders. Traditional accounting faced difficulties in reporting these transactions, and created differences between economic reality and actual accounting numbers. (Palepu & Healy 2003, 10-11.)

The mark-to-market accounting used by the company meant that once a long-term contract was signed, the present value of the future cash inflows were recognised as revenues and the present value of the expected costs were accounted as expenses. Unrealised gains and losses of these long-term contracts that were not hedged were, when they occurred, then reported as part of the annual earning. The main problem was in estimating the real market value of the contracts. Income was estimated as the present value of net future cash flows, even though the related costs and viability of the contracts were often very uncertain. (Palepu & Healy 2003, 11.)

Special purpose entities were used to fund or manage risks, which were related to specific assets. These special purpose entities are shell companies created by sponsors and funded by equity investors and debt financing. By 2001, Enron had used hundreds of these entities. Several of these entities were used to avoid some essential accounting principles. For example, Enron was able to avoid consolidating these special purpose entities to its financial reports, which resulted in Enron's balance sheet to understate its liabilities and overstate its equity and earnings. In 2001, Enron announced that to

correct its financial statements through the four year period (from 1997 to 2000) it would reduce its earnings by $613 million (23% of reported profits), increase its liabilities by $628 million (6% of liabilities and 5.5% of equity) and reduce its equity by $1.2 billion (10%). Due to Enron's high public debt and loss of investor confidence, in December 2001 Enron finally filed for bankruptcy. (Palepu & Healy 2003, 12-14.)

Enron's auditors, Arthur Andersen, received most of the blame for not recognising the problems Enron had in its accounting system. Arthur Andersen was in charge of reviewing Enron's compliance with the US GAAP and the company's internal controls. Instead, Arthur Andersen was accused of having shaky standards in their Enron audits, mainly because it was receiving significant income on consulting and auditing fees, therefore having a conflict of interest. For example, in 2000 Arthur Andersen earned around $52 million from auditing and consulting Enron. Finally when the investigations of Enron came public, Andersen attempted to cover up their involvement by shredding up evidence of supporting documents. (Palepu & Healy 2003, 18-19.) In 2002 Arthur Andersen was convicted of obstructing justice and the company is no longer functioning (Freifeld & Sandler 2010).

2.4.2 Lehman Brothers Holdings Inc.

Lehman Brothers was founded in 1850 in the US. After the US Civil War the company moved into New York and soon grew into one of Wall Street's investment giants. In September 2008 Lehman Brothers filed for the largest bankruptcy ever made in US history. The collapse sent global financial markets into a panic, pushing the global credit markets close to the edge. In 2010, the accounting firm Ernst & Young was sued for helping Lehman Brothers to "engage in a massive accounting fraud". (The NewYork Times 2012.)

It is said that the difficulties for Lehman Brothers began in 2007, as the mortgage market crisis around subprime and prime mortgages unfolded. In 2010, a chairman of the law firm Jenner & Block and a former federal prosecutor, Anton R. Valukas, published an examiner report on the bank. According to the investigations, Lehman Brothers had been using accounting gimmick to hide its true financial position. The

company was able to temporarily shuffle $50 billion of troubled assets off its books a few months before its collapse in 2008. This was to conceal its dependence on leverage, or borrowed money. According to Valukas, the company's executives and its accountants at Ernst & Young were aware of these transactions. (The NewYork Times 2012.) In the end of 2010, New York Attorney General, Andrew Cuomo, sued Ernst & Young for helping Lehman Brothers in a "major accounting fraud" (Freifeld & Sandler 2010).

According to Cuomo and Valukas, Lehman Brothers deceived investors and the public about its financials by using so called "Repo 105" transactions. These transactions are sale and repurchase agreements, or in other words, a form of short-term financing. Lehman used these to temporary move liabilities (in total as much as $ 50 billion) off its balance sheet to show that it was not carrying too much debt. Cuomo reveals that the Repo 105 transactions were initially reported as borrowings, but then in 2001 according to new accounting rules by Ernst & Young they were portrayed as sales. These of course gave a fraudulent impression on the company's leverage ratios and mislead its investors. (Freifeld & Sandler 2010.)

Ernst & Young, as the company's accountants, should have ensured that the financial statements complied with GAAP and were not misleading the public. Instead, according to Cuomo, E&Y knowingly helped Lehman Brothers to "manage balance sheet metrics". Nevertheless, the final responsibility should have been with the company's management, as even though financial reports may not be violating the US GAAP they can still be materially misleading. (Freifeld & Sandler 2010.) The investment bank faced a lot of lawsuits. For example, in August 2011, former officials of Lehman Brothers agreed to pay $90 million to settle a lawsuit accusing them of misleading investors about the company's financial situation in the months leading up to its fall. (The NewYork Times 2012.)

2.4.3 Fraudulent financial reporting in U.S. public companies

Fraudulent Financial Reporting: 1998-2007 – An Analysis on U.S. Public Companies was a comprehensive study, commissioned by the Committee of Sponsoring

Organizations of the Treadway Commission (COSO), done to provide better understanding of financial statement fraud cases. According to the study, from 1998 to 2007 there were 347 cases of fraudulent financial reporting in US public companies. In dollars the misappropriations accounted for nearly $120 billion in total of 300 fraud cases, which had the information available. The most common type of fraud detected was improper revenue recognition, which accounted for over 60% of the cases, following by the overstatement of existing assets or capitalization of expenses. (Beasley, Carcello, Hermanson & Neal 2010, iii.)

The study, first of all, revealed that fraud affects companies of all sizes. The organizations involved had median revenue and total assets just under $100 million in the period before committing fraud. The company sizes varied from startups to companies with over $100 billion in revenues, so it can be said that fraud is not limited to certain sized companies. 73% of the fraud companies' common stock traded in over-the-counter markets and were not listed in the New York or American Stock Exchanges. (Beasley et al. 2010, 2.)

In 89% of the cases the CEO and/or the CFO was associated with the fraud. According to the study, the common motivations for fraud included the need to meet earnings expectations, an attempt to hide the organisations worsening financial situation, the need to increase the stock price, the need to boost financial performance for possible equity or debt financing, or the desire to increase management level compensation based on the company's financial results. (Beasley et al. 2010, 3.)

One of the important insights made by the study was that characteristics between audit committees of fraud and no-fraud companies do not generally differ. For example, almost all of the companies investigated in the study had audit committees. These committees were in both company cases (fraud and no-fraud) groups of around three people and on average these groups met around four times a year. Therefore, it can be said, there is little evidence that the characteristics of the audit committees can be associated with fraudulent financial reporting. For what it comes to external auditors, it seems as fraud goes undetected by all types and sizes. 79% of the companies that had

committed fraudulent reporting were audited by the Big Four auditing firms. (Beasley et al. 2010, 3-5.)

After the Enron and Lehman Brother cases, in 2002 as a mean to prevent fraudulent financial reporting a new US legislation, called the Sarbanes-Oxley Act (SOX), was set forth. As the timing of this study includes only five years of the Sarbanes-Oxley Act – era, it is hard to give any valid conclusions on how it has affected the possible fraud behavior of companies. In particular interest is the Sarbanes-Oxley Act Section 404, which states internal control systems mandatory for all US companies. According to a Guide to the Sarbanes-Oxley Act, the summary of the section 404 is as follows:

> "Issuers are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures.
>
> The registered accounting firm shall, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting."
> (Sarbanese-Oxley Act 2002.)

In conclusion, after 2002 heavy legal requirements were set for US companies regarding the reporting on internal controls and the effectiveness of the related processes.

2.5 Internal control

Internal control can be defined as "a system of procedures implemented by company management. It is designed to follow objectives as: safeguard assets, encourage employees to follow company policy, promote operational efficiency, ensure accurate, reliable accounting records and comply with legal requirements." (Harrison et al. 2011, 237.)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is one of the main sources providing frameworks and guidance on enterprise risk management, internal control and fraud deterrence (COSO 2011). According to COSO's framework, internal control is an integral part of enterprise risk management. The role of internal control is to manage risk, rather than to eliminate it (KPMG 1999, 14). Therefore, before discussing the concept of internal control, we need to take a look at some facts and discussion related to risk management.

According to Collier et al. (2007, 10), risk management has been defined as the process of understanding and managing the risks that the organisation is inevitably subject to in attempting to achieve its corporate objectives (CIMA Official Terminology). The Institute of Risk Management has developed in 2002 a Risk Management Standard, which contains four elements: risk assessment, risk evaluation, risk treatment and risk reporting.

Risk assessment includes the analysis and evaluation of risk, by identifying, describing and estimating the possibilities. Risk evaluation is concerned with making decisions about the significance of the risks related to the company. So, whether or not the risks should be accepted, or should there exist relevant treatments or responses at hand. Risk treatment refers to the process of selecting and implementing measures in order to modify the risk. This can include risk control, risk avoidance, risk transfer, or risk financing. The final element, risk reporting, refers to the regular reporting on the organisation's policies on risk and the monitoring of the effectiveness of these policies. (Collier et al. 2007, 10-12.)

2.5.1 Internal control framework by COSO

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Internal Control – Integrated Framework* to help businesses and other entities with their internal control systems. Nowadays the framework is been used as rule, regulation and policy, by thousands of companies around the world.

During recent years, the concern over fraud and the focus on risk management have highly increased. COSO noticed a clear need for a robust framework to effectively manage risk. Therefore, in 2001 it initiated a project, along with PricewaterhouseCoopers, to develop an updated framework that would be readily usable by management. In 2004 the framework was published, and COSO believes this updated framework *Enterprise Risk Management – Integrated Framework* fills the need. This framework expands on internal control and provides a more broad focus on the whole subject of enterprise risk management. As mentioned before, risk management and internal control are closely related, and according to COSO internal control is incorporated within the framework of risk management. (COSO 2004, V.) This chapter will take a closer look at this *Enterprise Risk Management – Integrated Framework* (2004).

The ultimate assumption of enterprise risk management is that companies exist to provide value for their stakeholders. All companies face uncertainty, which presents both risks and opportunities. One of the biggest challenges is to determine how much risk a company is willing to accept while reaching for creating more value. Enterprise risk management should enable management to effectively deal with these uncertainties and trough this creates more value. (COSO 2004, 1.)

The goal of the enterprise risk management (ERM) framework is to enable companies to achieve their objectives. According to the framework the objectives can be viewed in the context of four categories: strategic, operations, reporting and compliance. (figure 5.)

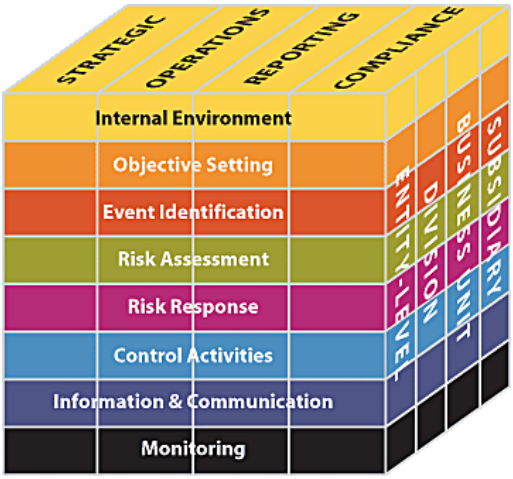

Figure 5. COSO Cube (IIA 2004, 7-8)

(1) Strategic: referring to high-level goals, which should be aligned with and supporting the company's mission. (2) Operations: effective and efficient use of resources. (3) Reporting: reliability of reporting. (4) Compliance: compliance with applicable regulations and law. This categorization makes it possible to have focus on separate aspects and it addresses different company needs. (COSO 2004, 3.)

The ERM framework considers activities from all different levels of the company: enterprise level, division or subsidiary and business unit processes. (IIA 2004, 8.) In front of the cube (figure 5.) the eight pillars represent eight interrelated components of the framework. These components are born from the way management runs a company and are integrated with the management's processes. The eight components are:

- **Internal Environment** – Internal environment sets the tone of an organization, and is the basis for how risk is viewed and addressed by the employees. This includes the philosophy of risk management and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective Setting** – Objectives are essential: through these management is able to identify potential events affecting the company's achievements. The chosen objectives should support and be in align with the entity's mission and be consistent with its risk appetite.

- **Event Identification** – Internal and external events affecting achievement of objectives need to be identified, and determined as risks and opportunities. Opportunities should be channelled back to the management's strategy or objective-setting processes.
- **Risk Assessment** – The likelihood and impact of risks are analysed, in order to determining how they should be managed.
- **Risk Response** – The management needs to select how to respond to the risks: avoid, accept, reduce, or share the risk. This means developing a set of actions to align risks according to the company's risk tolerances and risk appetite.
- **Control Activities** – To ensure that risk responses are effectively carried out, procedures and policies need to be set out.
- **Information and Communication** – Relevant information needs to be identified, captured, and communicated in a manner that employees can carry out their responsibilities. Effective communication is as well flowing down, across, and up the organisation.
- **Monitoring** – The company's entire enterprise risk management needs to be monitored, and if necessary modifications should be made when needed. The monitoring happens through management activities and/or separate evaluations.

All of the components mentioned above are interrelated, where almost every component has an influence on another. The cube (figure 5) describes the relationship between the eight components, the entity's units and the four objectives in a three dimensional matrix. The objectives are represented in the vertical columns, the components in the horizontal columns and the business units in the third dimension. (COSO 2004, 3-5.)

For a company to have effective ERM the eight components need to be present and functioning. No material weaknesses can exist and all the risks need to be taken into consideration in the risk appetite, in order for the components to function properly. However, one must bear in mind that the eight components do not function identically in all organisations. For example, in smaller organisations they may be less structured and more informal, but still effective. Despite the benefits of ERM certain limitations

do exist. As the operators of the system are merely human, mistakes and errors are naturally a part of so called human failures. (COSO 2004, 5.)

2.5.2 Internal control guidelines by KPMG

Many companies have created their own internal control systems, however they tend to follow the principles set by COSO. To take an example, the report will take a closer look at one of the leading auditing companies' system. The KPMG guide, presented in this chapter, links the theoretical concepts a bit more into practice, and therefore beneficial to take a look at.

As the business world is constantly changing, and the companies live in a turbulent environment, a successful internal control system also needs to be open for changes. Effective risk management and internal control therefore need regular evaluation of the nature and extent of risks. The ultimate responsibility of the internal control should be with the board. This also means that the board should be the one sending a clear message to the whole organisation that the responsibility of internal control should be taken seriously. (KPMG 1999, 18.)

In order to have an effective system of internal control, the board should consider the following aspects (KPMG 1999, 19):

- the nature and extend of the risks facing the company
- the extent and categories of risks which can be acceptable for the company to bear
- the likelihood of the risks which concerned materialising
- the company's ability to reduce the incidence and impact on the risks that do materialise
- the costs of operating particular controls relative to the benefit, thereby managing the related risks.

Following COSO's framework of internal control (Internal control - integrated framework) published in 1992, KPMG also comprises the same common elements to

its system: control environment, identification and evaluation of risks and control objectives, control activities, information and communication processes, and processes for monitoring the effectiveness of the system of internal control. Figure 6 below represents the five different components mentioned, with the board as the centre of all. (KPMG 1999, 19-21.)

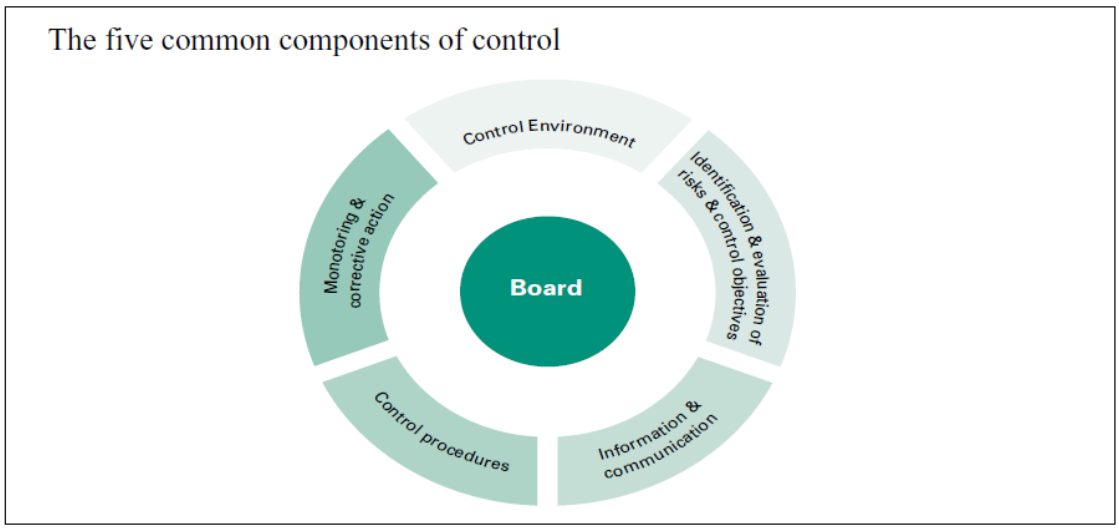

Figure 6. The five components of control (KPMG 1999, 22)

However, it is not enough only to have all the components present, it is also important to understand the nature and the context of the control. First of all, as control should be capable of responding quickly to evolving risks, it is important to get the control as close to the risk as possible. The company needs to have the capacity to respond and adapt to unexpected risks and situations, and to make decisions despite having all the information. This is why the control needs to be close to the associated risks - the shorter the chain, the quicker the reaction. (KPMG 1999, 22.)

Secondly, the costs of the control need to be in balance against the benefit of controlling the risk. As it may happen that the cost of additional control becomes greater than the actual benefit arising from the controlling of the risk. Thirdly, the control system needs to include reporting procedures, which communicate immediately to the right management levels of any significant control failings or weaknesses that are identified. The reporting should include also details of the actions being undertaken. This also means that the philosophy of control should come from

the top of the company, with an emphasis on continual learning, instead of a blaming culture.

Even though control can minimize errors and risks, it cannot for sure provide absolute assurance that they will not happen. Nevertheless, it would be important to blend the control system in the company's operations and have it as a part of the company's corporate culture. As a company is run by individuals, the control system is affected by people throughout the company. By making these individuals, so all the people in the company accountable, the likelihood of an effective control system is increased. (KPMG 1999, 22-24.)

KPMG has developed a Risk Management Diagnostic, to help organisations follow whether all of the necessary components for an efficiently working internal control system exist (figure 7). The diagnostic has been visualised as a triangle, representing seven components, and relevant questions under every title for managers to consider.

Philosophy and policy

- Is your organisations risk management philosophy and policy clearly defined, communicated and endorsed by the board?
- Are there clearly defined roles and responsibilities for the identification, management and reporting of risk?

Behaviour

- Are those responsible for risk provided with appropriate formal training?
- Does the organisation learn from the risk events when things go wrong rather than seek retribution?

Roles and responsibilities

- Is the responsibility for reporting clearly defined?
- Are responsibilities written into all relevant employee job descriptions?

Demonstration of performance and risk effectiveness

- Is the board provided with a clear picture of performance?
- Are KPI's clearly defined and measured?

Converting strategy to business objectives

- Do business objectives reflect strategy?
- Are business objectives clearly communicated?

Performance appetite

- Is your organisation's risk appetite explicitly and clearly defines?
- Are action plans developed to move the organisation to a more desired risk profile?

Risk to delivering performance

- Does the risk information assist management in identifying accumulations and dependencies?
- Are management actions and controls identified and monitored for the risks?

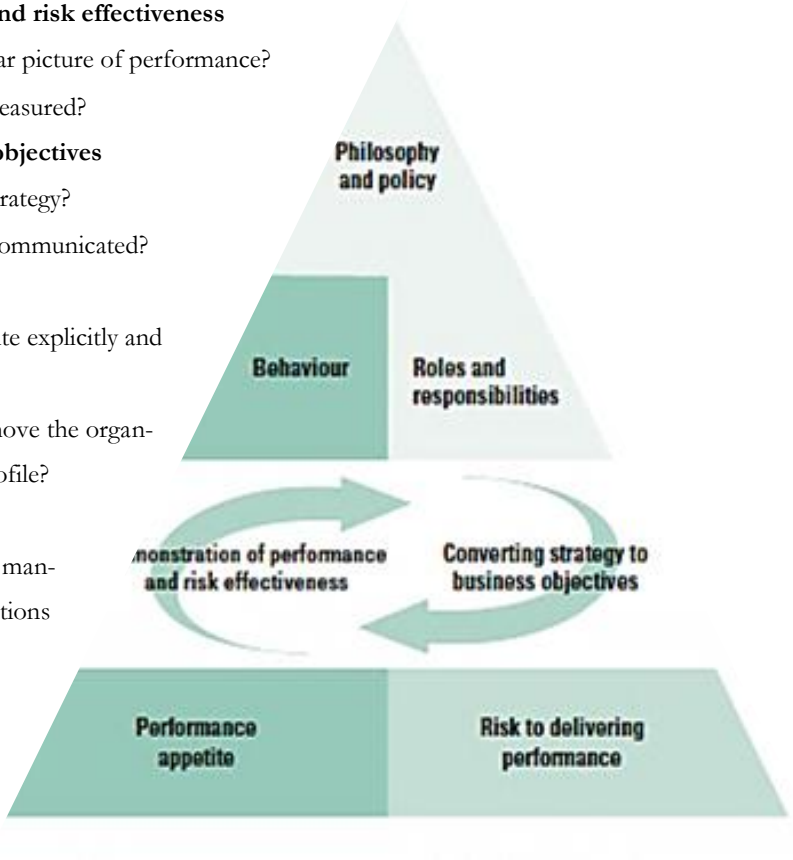

Figure 7. Risk Management Diagnostic (KPMG 1999, 25)

In addition to the Risk Management Diagnostic, the triangle above represents the framework companies should use to assess the effectiveness of their internal control system. KPMG believes that for any control model to work effectively and be relevant to the performance of the business, it must contain these key components.

Starting from the tip of the triangle, **Philosophy and policy**, represents how the board should make the risk management expectations explicit. Employees need to know what is expected from them and what is not. **Roles and responsibilities** represent the importance of making all the roles and responsibilities of the key performers explicit. **Converting strategy to business** objectives includes the idea of making strategic and business objectives explicit. This way the likelihood of overlooking significant risks will be reduced, as the link between strategy and business planning is a critical risk management process. **Risk to delivering performance** refers to how the significant business risks should be formally identified by the board and this way show that they are aware of the possible risks. In the left bottom of the pyramid KPMG has **Performance appetite**. This means that the probability of the risk of occurring and of the impact of that risk should be analysed. The cost and benefit relations need to be analysed as well. **Demonstration of performance and risk effectiveness** refers to how performance should be monitored against targets; an assessment of the effectiveness of the control should periodically be provided to the board. This process has some circularity, as monitoring may lead to re-evaluating the company's objectives or control. Finally, the triangle has **Behaviour**, which represents shared ethical values. These values, including integrity, authority, responsibility and accountability, should be established, communicated and practiced around the whole organisation. (KPMG 1999, 67-68.)

Some of the most common weaknesses in organisations happen with (KPMG 1999, 26):

- **Philosophy** – it is understood, but not written, so it is open for misinterpretation
- **Roles and responsibilities** – the responsibilities are not clear throughout the organisation
- **Converting strategy to business objectives** – strategic objectives are not directly business objectives
- **Risk to delivering performance** – a form of risk profiling, but often differs from the reality of doing business

- **Performance appetite** – missing the understanding of the organisation's risk appetite
- **Performance and risk effectiveness** – boards do not receive the right information, so either too little or too much
- **Behaviour** – disincentives exist which lead employees to behave in a non-functional manner.

3 Research methodology

Mostly qualitative research has been done. Historical data has been collected by doing desktop research, as there are a lot of different sources discussing the topic of internal control. The field research that was done for the report included a survey and interviews.

3.1 Research design

The research definitely needed to begin with researching the background, different theories and earlier studies. This helped to formulate clearly what needs to be found out from the survey and interviews, and therefore enabled creating the survey and the interview framework. First, the Webrobol survey was developed. The sample selection, so for whom the questionnaire would be sent to, was collected by contacting the Big Four auditing companies by email, and simply asking for suitable employees' contact information. It was determined that the respondents should have relative knowledge on internal control, in order to give insightful answers to the survey. After going through the questionnaire answers and doing an initial analysis, the research process could continue to the interviews. The same four auditing companies were contacted, after which specific dates with the companies and the interviewees could be agreed upon. The next step was to collect the relevant data from the interview records and analyze it. Finally conclusions can be made and a discussion on some possible development suggestions (figure 8.)

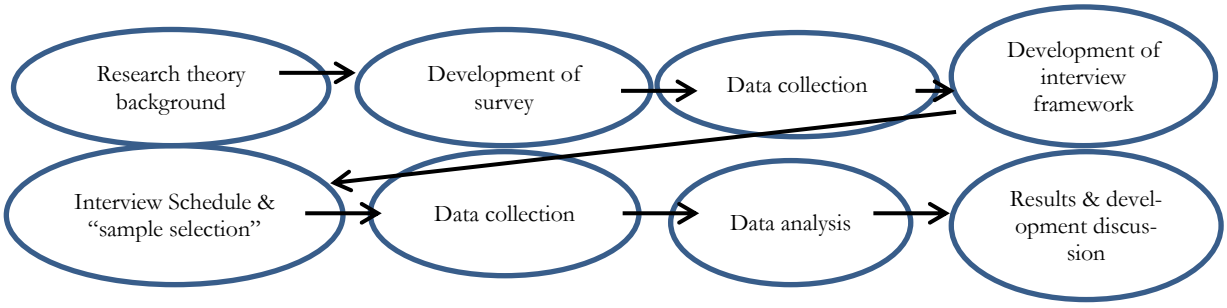

Figure 8. Image of research design

3.2 Research process

The research process is divided into two main parts, beginning with the survey and then proceeding to the interviews. The actual research process began during spring 2012 and continued to the beginning of 2012 autumn. The following chapters will describe the processes in more detail.

3.2.1 Survey

The survey on internal control and fraud was sent to 19 persons working in the Big Four auditing companies: KPMG, Ernst & Young, Deloitte and PricewaterhouseCoopers. The sample group represents managers and employees, who have a relatively high knowledge on internal control. And therefore, should be able to answer the survey with deeper understanding and knowledge. The sample selection took place by first contacting each company by email, and inquiring for possible candidates to respond to the survey. The initial contact persons from the companies were found from the organisations' Finnish web-pages, and selected based on their positions: either employees or managers working with risk management and/or internal auditing. The four organisations each provided one to five possible respondents to answer the survey.

The survey was published on the 10th of May 2012 and sent to the sample group via Webropol, which uses emails providing a link to the survey (attachment 1). During a one-month period, despite five reminder emails, only six replies for the survey were received. Half of the respondents were senior managers and the rest included a public accountant, director and an owner/partner. Due to the low answer rate, no valid conclusions or generalizations can be made only based on the survey. However, the answers do give some direction for the research, and a good source of background information for the interviews discussed in the next chapter.

3.2.2 Interviews

The interview framework was developed after collecting the data from the survey answers, in the late August 2012. The interview questions were developed to give more

depth and detail to the research, by keeping the survey results as a baseline, were could be built on. During September 2012 three face-to-face interviews were conducted. Due to privacy reasons, the interviewees will stay anonymous and from here onwards referred to as Interviewee 1, Interviewee 2, and Interviewee 3.

The most appropriate approach was to conduct thematic interviews. A thematic interview, according to Hirsjärvi & Hurme (2008, 47), includes questions, determined by the interviewer, which have been formulated prior to the interview. However, the actual interview is freer and more fluent than a structured interview; as the questions do not need to follow a certain order, and the answers cannot really be strictly categorized into any predetermined options, and therefore the interview resembles a conversation. A thematic interview takes into consideration very essential issues, such as the interviewee's way of interpreting topics and the focus that they bring to the different issues. It can be said that the thematic interview approach gives the interviewee a voice. (Hirsjärvi & Hurme 2008, 48.)

The initial plan was that the interviewees would only include representatives from the same Big Four auditing and consulting companies, who had responded to the survey. However, a good example of a recent fraud case came across, and an opportunity to interview the company's financial manager about it. Therefore the interviews were conducted as follows: two interviews with representatives from the Big Four and a third interview, which was to represent a company case of experienced financial fraud. The same interview framework was used in all of the interviews (attachment 2). All of the interviews took place in the companies' Helsinki offices, and their durations varied from 30 to 50 minutes.

4 Data collection

The primary data has been collected by a survey and interviews. A Webropol survey and a thematic interview framework have been the tools used for collecting the data. As an addition to the survey, the interviews give a deeper insight and personal answers, and therefore provide relevant findings concerning the topic.

4.1 Survey

To have some structure, the survey was divided into four sections, beginning with a few questions on the background of the answerers. All of the respondents have more than five years of experiences in the field of financial auditing and five out of the six had ten or more years of experience. Using a Likert scale from one to five, one representing poor and five excellent, the respondents graded their own knowledge on internal control with an average of 4.5. Based on the above information, it can be said that the data collected from the survey is answered with experience and therefore is reliable.

4.1.1 Roles, responsibilities and decision-making

The actual first part of the survey included questions on roles, responsibilities and decision-making. All of the respondents were well or very well aware of their own role and responsibilities in their company. However, it seems that in most of the cases, no concrete responsibilities are written to the employees' job descriptions. Either they have been written in general level or then there exists only project specific written objectives and tasks. When asking about, how often does the respondents' responsibilities require only their decision-making, it is clear that most of the respondents are higher-level managers, as this level decision-making is required often or even daily. Even though it seems obvious that the leader, or the person in the position of a manager, is required and expected to make decisions solely, in terms of internal control it can, however, be questionable.

4.1.2 Controlling the company – Current internal control system

The timing of implementing internal control systems differs among the four companies, but it seems that policies and guidelines defining aspects of internal control have existed from the start. According to one of the respondents, the most recent methodology they apply is about 2-3 years old. And as according to most of the guidelines on internal control, this is under continuous development to ensure that they also apply the relevant guiding principles in an efficient and effective manner. Another respondent answered that their company implemented their system in 2008. These two answers would suggest that in the past few years the topic of internal control has been brought up again.

To have an effective internal control (IC) system, the objectives of the system need to be clear and specified. From the survey we can see how companies' IC objectives vary from general to more specific. According to respondents, their IC objectives include:

- compliance, reputational risk management, integrity, financial reporting
- ensure compliance with internal policies and procedures, ensure that brand reputation is not harmed
- 1. reaching of objectives and making sure strategy is implemented, 2. management of risks related to the business, 3. securing that laws and regulations are complied with
- protect the firm and its brand from the risks that arise in its professional practice
- to assure that the risks relating liabilities are systematically and well managed
- ensuring achievement of objectives and with regards to client work that the quality and integrity in everything we do is not compromised and that we apply ethical considerations in all our decisions and actions.

Based on these very thorough answers to this question, it seems the objectives of the internal control are clearly defined and understood by the respondents.

According to the theory, risk management and internal control should be directed, coordinated and monitored by the board. Questions nine and ten where to find out, who in practice is in charge of these risk management and internal control operations. Even though the questions are asked separately, the answers seem to repeat their selves. As a summary, management and the Board of Directors seem to be the ones ultimately in charge. They are the ones responsible for implementing a proper system of internal control, and the management is then more in charge of ensuring that the system is put into effect. However, in both cases one respondent adds that "all personnel" is in charge. This of course is something that one should also bear in mind that even though the instructions come from the top, everyone is personally in charge of their own behavior.

All of the respondents were aware of the nature and extent of the risks facing their organization. This, according to the guidelines represented by KPMG, is one of the first points that make an internal control system effective. This question and examples of risks were also asked during the interviews, so this will later on be discussed in more detail.

The objectivity of an internal controller plays a significant role when it comes to monitoring and assessing the effectiveness of the controls (Glader, H. 24 Apr 2012). Therefore, question 12 from the survey asks specifically about the internal controller, and whom he or she works for, i.e. is he an employee from the organizations payroll or hired out-side the company. The answers varied a lot. Three responded with not having such a specific role at all, two said that the person is hired internally and one responded by having both. One of the respondent, who referred to not having one separate internal controller, brought up a new aspect of having a so-called grandfather principle instead. This is used when monitoring the most important areas and done by many levels over the organization. In the organization, which was referred to as having them both options, described that the finance and IT departments perform some of the controlling tasks, and then the outsourced functions perform controlling tasks such as travel and expense reimbursement handling.

Internal audits, according to 3/5 of the respondents, are held annually. One replied every three years and the last said that responsibilities are divided inside the organization, which probably would refer that different divisions organize them according to their own needs.

The purpose of an internal audit is to monitor and evaluate how effectively and efficiently the internal controls and risk management are followed. In addition the implemented systems need to be in align with the objectives that have been set. One of the internal audit's outcomes could be that some possible risks are detected. In this case the board and management should take action, by evaluating the depth of the risk and then accordingly add possible new procedures for the system. All of the respondents gave a similar answer: as a summary, corrective actions are taken and the processes are updated accordingly. In addition, one of the respondents referred to an interesting point, concerning severe risk management violations. Severe violations have a direct impact on a person's performance evaluation and hence compensation. So the employees are given a so-called carrot, to provide motivation, to properly follow the implemented control procedures.

The main reasons for implementing an internal control system is to improve a company's performance and prevent fraudulent behavior (attachment 1. questions 16-18). Three of the respondents commented on how exactly the controls improve their performance, and it seems that all of these four auditing firms consider internal control as a necessity. According to the answers, the control procedures for example, provide high-quality service seamlessly on a global basis, set standard operating principles and ways of working according to policies and guidelines, which brings efficiency, and keeps employees sharp with regards to the internal activities. In addition, the different control activities make accurate, relevant and timely reporting possible. Only 1/3 felt that their company's internal control system highly prevented fraud. However, from the scale of one to five, number one representing "not at all" –prevention, and number five representing "high" –prevention, all of the respondents replied with number three or above. This would suggest that internal control does play a role in preventing fraud, however not 100 percent.

As discussed in chapter 2.1 people conducting fraud can be observed or analyzed through the fraud triangle. For an ordinary person to commit fraud, there needs to be the three elements of motivation, rationalization and opportunity in place. The internal control system should be the procedures, which exist in order to prevent the element of opportunity to take place in this equation. Therefore it was relevant to add this question in the survey. According to the respondents, it seems the opportunities to conduct fraud are the same for managers and employees. None of the respondents answered that no opportunities would exist. However, 50% replied that for both cases, management and employee, the opportunities for committing fraud are below moderate. This suggests that fraud is something that can be done; however the systems are controlled in such that not many opportunities exist.

4.1.3 Board meetings and relationships

According to most of the respondents, the board reviews their company's risk management and risk analysis annually. However, for what it comes to the actual internal control system, most of the respondents (66%) were not aware of how often this is done. Only two of the respondents replied that this is done annually. Based on this no greater generalizations can be made, nevertheless it can be interpreted in such as that employees are more aware of their company's risk management processes then the ones related to internal controls.

As a quite new trend, companies are being looked at and evaluated based upon their transparency, relationships with stakeholders and integrity. The respondents' replies varied quite a bit, when asked about transparency over relationships with stakeholders. Using the same scale, as before, from one to five, one out of four replied that the transparency is high, two responded it being over moderate, and one under moderate. As all of the respondents are representatives of high quality auditing organisations, this might just implicate that transparency is viewed differently. As said by one of the respondents: "a client cannot be a stakeholder; independence is secured in all cases". For what it comes to controlling relationships between clients and other stakeholders, one respondent clarifies that in their organisation they need to submit an annual web-

based statement concerning the employee's knowledge on the relevant guiding principles related to client and stakeholder relationships. According to the same respondent, all employees have the responsibility to apply related principles when dealing with clients and other stakeholders.

Often old employees possess a lot of confidential information about the organisation and its clients. Therefore after an employee resigns some regulations are in place. Some examples of regulations were asked, and the respondents brought up a few: laptops are owned by (and returned to) the company, non-disclosure clauses exist on confidential information, and possible physical restrictions exist as well. The information received during the employment needs to be left to the company and it cannot be used afterwards.

4.1.4 Fraud

The final part of the questionnaire included questions specifically related to fraud. As the topic of fraud is quite delicate, not too revealing answers could be expected. However, the respondents had unexpectedly very little to answer for this whole part of the survey. According to the respondents in three out of five of the case no fraud related cases had happened in their organisation's history. Two answered with a "maybe", sadly however, this does not give any additional insight to the topic.

As a researcher, it was only at this stage obvious that the topic of fraud should have been approached differently, for actually receiving some more depth and content from the respondents. For receiving more data and validity to the topic, especially to the aspect of preventing fraud, the interviews were in place. Therefore this will be discussed in more detail in the following chapter.

4.2 Interviews

The thematic interviews could basically be divided into three sections according to the themes. According to Aaltola & Valli (2001, 143), this is the first step to be done when unfolding data from thematic interviews. The classification of the data makes

conclusions possible, as it provides a clear framework, which can be followed (Hirsjärvi & Hurme 2008, 147). Before going to the actual topic of the research, a few questions on the interviewees' backgrounds were asked. All of the three respondents have a long experience in their fields of expertise, and all of them had worked in their current organizations for over ten years. In the following chapters, the interviews will be discussed from two different points of view: one from the company case point of view (Interviewee 3) and the other from the so-called expertise's point of view, referring to the auditing & consulting companies (Interviewee 1 and 2).

The representatives from the two auditing companies have both been working with risk management in the same company for over ten years. Both of these interviewees have management positions and act as supervisors. Interviewee 3 is the financial manager of the company, with 35 years of experience working in the same organization. Due to the long working histories in the same field, it can be said that all of the interviewees have a reliable knowledge and personal experience in risk management, and in more precise also in internal control.

Table 2 represents a brief overview on the three interviews. The themes have been categorised under three main topics: risk management, internal control and fraud, and under each topic one can see the main points brought up by the interviewees. The following chapters will discuss the topics in more detail.

Table 2. Overview of the interviews

	Risk management	Internal control	Fraud
Interviewee1	• comprehensive quality risk management • importance of brand and quality • client risks	• processes begin from planning: strategy, operations & budgeting process => in align with international group • continuous reviews for client engagements • monitoring from India • following internal control processes a part of employee remuneration	• worked with fraud cases • believes that most go un-noticed, however generally people are decent and honest • often starts small and escalates • example situation: money trouble + opportunity = fraud
Interviewee 2	• risk and reputation management • value control • client risks	• code of ethics, ethical instructions & independency regulations • regular reporting to global group • employees trained and tested on knowledge • internal audits every three years, include question batteries related to the global requirements	• worked with fraud cases • more damage vs. benefit • cases mostly related to monetary transactions • companies don't realise the risks • example situation: cost friendly loan decisions for friend
Interviewee 3	• different approach, as part of the business is to take risks • categorisation under three titles; operative, reputation, and strategic risks	• avoiding dangerous working combinations • controls in IT programs, e.g. user ID's • internal controller & external auditors, conduct audits: processes & financial statements • board meetings & continuous development • reporting on "nearby" situations • blaming culture slowing the development	• personal experience of colleague committing fraud • fraudulent financial transactions from the company's account to personal account • led to changes in control processes • afterwards loss of 30 000 € retrieved • left colleagues with feelings of betrayal and disappointment

4.2.1 Risk management

All of the interviewees emphasized on the comprehensiveness of their risk management. The auditing companies both had reputational and quality issues in high importance, as they referred to "comprehensive quality risk management" and "risk and reputation" management; where the quality or reputation is already included in their internal terminology. This of course seemed to be because of their delicate businesses, and the requirements that have been set forth by the companies' global groups. Both Interviewee 1 and 2 explained that most of the risk management aspects are related to so-called client risks. The selection of customers seems to be in both of these companies highly regulated and monitored. The companies emphasize in bringing value to the customers, but at the same time the customers should be trustworthy, for example, what if comes to financials and the ability to perform payments. Ultimately, the brand and reputation need to be protected and kept in high quality.

The Interviewee 3 had a quite different approach, as the business differs quite highly from the auditing companies. One relatively central part of the business is to take risks, and therefore when talking about risks one should remember the opportunities that arise from risk taking. Nevertheless, the company categorizes their risks under three main titles; operative, reputation, and strategic risks. Strategic risks can further be divided into financial risks and business risks, all of these however are highly interrelated.

All of the interviewees seemed to be fully aware of the nature and extent of risks facing their company. The risks discussed could be divided into internal and external, coming from the operating environment and from the macroeconomic variables. Starting from the big picture, all general economic developments have an effect on these businesses. Especially for an auditing company, an economic downturn decreases the demand for consultancy services, which as usually among the first things to be cut. On the other hand, economic crisis or financial crisis can also create opportunities: when living in uncertainties companies experience change and transformations, which often require

outside assistance. This is yet another reason why risks are not only downsides, but also opportunities.

Some business level risks are mostly related to regulations, which arise mainly from the European commission or other regulatory bodies. One example of these regulations could be the EU green paper. Competition, in regards to profitability, can as well be categorised under business level risks. Both of the auditing companies also mentioned the importance of their brand's value. Risks exist with engagements and new clients, therefore reputation risk is very highly taken care of and the brand is not risked, for example with badly evaluated client engagements. Internal risks can include issues related to efficiency for example; how to find the right know-how to the right customers and projects. Especially, in situations where tasks are related to some very detailed and precise knowledge, as it seems that very little of "niche" –knowhow exists. The situation requires an increase in education for employees, which would entitle a situation where efficiency and capacity would be in balance.

4.2.2 Internal control

As Harrison et al. (2011, 237) define internal control as "a system of procedures implemented by company management" it was interesting to hear what kind of processes are these in real life. According to the representatives of the Big Four, the processes can be divided into different parts. According to Interviewee 1, their company's processes already start from the planning stage, which includes the whole strategy process; operational planning and the budgeting process. This is to secure that all the business units in all the different geographical areas are in align with the group's strategy. As the ultimate goal of control, is that the organisation meets the strategic goals and objectives that have been set by it. Processes that come across in daily work are highly related to the client risks, as the business consists mostly of project based work. A few examples; before accepting a proposal, the company, or in more specific an auditor, needs to consider whether or not they can meet the clients' expectations, to assure quality delivery. For certain projects client satisfaction is measured. After the project is done, to get an objective overview the client is interviewed by an

independent person from the auditing company, so a person who has not been engaged in that specific project.

According to Interviewee 2, centralized instructions and guidelines on reputation and risk management come from the group, and need to be followed world widely in all of the international offices. These instructions include the code of ethics, ethical instructions, and independence issues. All of these issues need to be reported to the higher organ regularly, the independence when working with customers in this business is of high concern. The regulations also include topics on anti-corruption and money laundering. In the interviewees own unit, employees are trained to the topics mentioned above, and regularly tested on their knowledge.

Interviewee 3 looks at the topic from the operative risks point of view, and finds that avoiding dangerous working combinations is one of their main tools used when it comes to internal control. This in practice could mean, for example, regulations on who has the right to accept different matters. This can often be part of the IT programs, for example, the user identification codes (ID's) can be determined so that different employees can access only selected information. The user ID's also allow the management to follow logs, where one can see what a certain employee has been doing. According to the CFO, they take random spot checks to monitor the efficiency of the controls. A crucial step in the processes of the financial department happens often with the handling of the bank accounts and payments.

The interviews concentrated next to the actual practicality of the internal audits; how often and what are some of the basic elements included in an audit. The interviewees presented different approaches, however the same basic element could be detected from all of them. The audits are done at different levels and no-one reviews their own work. Interviewee 1 refers to their continuous audits as reviews; these are done of individual client engagements. Higher level monitoring is conducted from the group's Indian office. They monitor that the risk management procedures have been followed, and both the clients and engagements have been selected accordingly. Doing this remotely is possible, due to the global information systems the group possesses. The

engagements are also locally reported on, as reports concerning the status of quality and risk management procedures are obligatory. Interviewee 2 explains how their internal audits are done every three years. These audits include questionnaire batteries related to the global instructions. The strictness of the compliancy with the global guidelines is every time higher, meaning that the company is expected to have improved for every audit. After half a year from the audit, the audited company needs to report its improvements regarding the compliancy with the regulations.

Interviewee 3 explains their internal audits as follows. The company has a designated internal controller, who is independent and works under the CEO. The company also has external auditors, who conduct audits twice a year. According to the interviewee nowadays the auditors highly concentrate on the actual in-house processes and the steps on what have led to the results. It seems that the auditors trust the results if they are satisfied with the processes. Before an audit, the auditors consult the internal controller on what she has already audited, so the same area is not audited unnecessarily multiple times. The auditors conduct one audit related to the processes, which is done during the autumn, and another one related to the financial statements is done during spring. Other practical processes related to the internal control system are board meetings and a part of them continuous development. The risk management board meets up with representatives from all of the departments, and together they discuss development suggestions and improvements. An example of a current development suggestion has been with reporting on "near or almost" - situations. According to the company's guidelines on internal control, all risky (near or almost) situations should be reported to the board, as well as all the risks or mistakes that have realised. To actually make this happen the organization culture and atmosphere should be more open. Currently it seems there is too much of a blaming habit in the air. The change of course should come from the management, who should change the philosophy with regarding to this and open up the atmosphere. When the blaming is left out, everyone could be able to learn from the mistakes, and then go forward with more wisdom. Currently the company is going through a transitional stage regarding this.

None of the three interviewed, can straightforward pinpoint any possible failure points in their internal control systems. However, an essential part of the systems is continuous development and improvement. More and more practical processes and automation have been included. And as the value of the controls is understood, there is less resistance. It seems that in the past few years a lot of companies have taken big leaps in improving their control systems.

Legally, none of the companies are obligated to report on their internal control in specific. Nevertheless, all of these three companies do report on it in one way or another. According to Interviewee 1, they are required to report to their India office, which takes care of monitoring their processes. However, he adds they could be more transparent about their internal control procedures, as especially clients often ask about how risks are managed within their organisation. Interviewee 2 can only say about the Sarbanes-Oxley Act, which is required to be followed in the US based subsidiaries, however something with similar precise legal reporting requirements does not exist in the Finnish office. According to Interviewee 3, their company needs to follow multiple laws and regulations related to reporting in their business. Most of these are guidelines related to risk management, and they are determined by the Finnish Financial Supervisory Authority. A positive thing is that the company wants to report on the risks and controls as widely as possible, for example they have in their annual financial statements a chapter on risk management. The Financial Supervisory Authority has full access to all the reports and information related to risk management, and also within that everything related to the so-called nearby situations.

As presented in chapter 2.5.2 in the Risk Management Diagnostic developed by KPMG (1999, 25), the communication and philosophy on risk management as well as internal control should come from the board. Therefore the interviews also touched the topics of communication and organisational philosophy as well as culture. According to Interviewee 1, their quality risk management (QRM) covers the communication and reasoning on why certain procedures are done and why they are important; this is done by providing a lot of training material to the employees. Interviewee 2 explains how a part of their communication methods includes an

annually conducted web-based survey regarding the independency of engagements, plus some compulsory e-learning on ethical issues is required. The depth of the independency questionnaire and the required learning vary based on the employee's position; there are higher requirements for the management. These answers are then reported to the head of the global organisation. For what it comes to attitudes, many seem to consider the surveys quite heavy and long, but understand the importance of them.

In Interviewee 3's company a risk management plan is updated and published every year. More detailed risk management education is given for all the supervisors, who should then communicate it and the philosophy behind it to the rest of the employees. Currently an issues under discussion, is which kind of realised risks/nearby situations, should be reported on, and to whom and until what level. The aim would be that everything should be reported on, in order to discuss and improve the control processes. The difficulty seems to come with the optimization, as not everything can be determined in money it makes it hard to describe what kind of issues are relevant to report on. For example, it is difficult to give monetary value for reputation, but the risks related to it can create tremendous loss.

For what it comes to the general view on internal control among the employees, the interviewees had quite similar answers. People are well aware of the importance and understand why things are done as they are. Some negative factors relate to the bureaucracy often required to fulfil the processes. Interviewee 1 brings an interesting fact about their processes related to internal control: a part of their remuneration program involves the fact of how well the quality and risk management have been carried out. In other words, following and reporting on the QRM is a requirement for a bonus; if not doing well in these aspects, the employee does not receive a bonus. Interviewee 3 refers to their corporate culture as careful and responsible. The bureaucracy and stiffness comes across with some IT programs and systems. Employees sometimes feel these different controlling methods are often not easy to operate with and they can slow down the processes.

The final question of the interviews was: is there a need for an internal control system in every company, and/or could there be any negative factors of having an internal control system? All of the interviewees agreed that an internal control system should be a part of every company's risk management. However, the extent of the control system should suit the organisational culture and be in proportion with the size of the company. For example, both Interviewee 1 and 2 would consider the US SOX reporting system too strict to be used in Finland. According to Interviewee 1 the SOX legislation has brought negative reputation around internal control, as the reporting requirements brought a lot of laborious and troublesome work for companies. Interviewee 2 explains that a too hierarchical system can often slow down the processes, and too intense micromanagement that is not necessary, is also not beneficial for the company.

4.2.3 Fraud

The two interviewees from the auditing companies have come across and worked with cases related to fraud, due to the nature of their work. According to Interviewee 1, most of the cases however do go un-noticed. Recently, as these fraud cases keep popping up, companies have become more and more interested in implementing higher controls. Generally speaking, Interviewee 1 believes people in this culture are decent and honest employees, and from the ones who have committed fraud, 80% have no criminal records in the past.

Often the suspicion of fraud and the impulse to investigate it comes from the company, which then leads to an audit and a possible confirmation. The fraudulent behavior has usually only been related to something quite small and foolish. For example, paying bills to personal bank accounts, leads to more damage than benefit for the employee. Interviewee 2 explains how the cases have mostly been related to monetary transactions, and the control risks are usually related to employees' having access to the payment programs in the company's systems. Companies often don't even realise the risks that are involved.

Interviewee 3 told in detail about a fraud situation his company had experienced recently. The fraud was one of the most common types of corporate fraud: misappropriation of assets. The misappropriation of assets continued for one year, with building to a monetary value of around 30 000 € in total. The employee was able to transfer money, intended for paying the company's bills, to her own account and also to some other account registered under a "hobby club". Monthly the transferred money was only around one thousand to up to five thousand Euros at a time. The employee had worked in the company for 30 years, but something happened during the last year. There might have been some personal issues in the background, as according to the interviewee, the employee had acted strangely for the last one year, before gotten caught. During that specific year, the actual team leader, under whom the employee who conducted the fraud had worked for, was on her maternity leave. This team leader noticed the fraudulent transactions, after she came back from her leave; she first wondered why some transactions had been made double, and why some of the records seemed unclear. The employee was able to go around and explain some of the records, but finally the person got caught of the wrongdoings when a customer called and asked about a missing payment that had been due. This led to deeper investigations, which revealed that the employee indeed had fiddled with the systems and changed some of the customers' the bank account information to her own account.

The employee got caught on a Tuesday and finally, after waterproof evidence, fired within a week. The final criminal verdict is yet to be announced, but the monetary losses have been retrieved. As a consequence after this case there have been a lot of changes in the company's IT processes, settings have especially been changed so that the person who is able to change the account numbers, is a different person who fills-in the actual monetary transactions. In other words, more bureaucracy and controls have been added to the processes.

In addition to what have been mentioned, the whole situation had a huge effect on the other employees as well, as it brought up feelings of disappointment, betrayal and shock, especially as the person had been a long-lime trusted employee. To tackle all the

personal issues among the colleagues, the company organised a group discussion, plus personal discussions with a psychiatrist, in order for people to get past the shock and continue work. Nevertheless, the fraud case seemed to bring doubt and distrust among the rest of the employees.

None of the interviewees were able to pinpoint some clear reason for people to commit financial fraud. According to Interviewee 1 the so-called fraudulent behaviour often starts small and then later on grows. The specific employee might be experiencing financial trouble and then if an opportunity comes along, the motive and reasoning comes easily as well. Interviewee 2 gave an example of a situation where the person committing the fraud, did not actually benefit anything, instead he was just helping a friend. In this example of fraud, the employee worked in the financial sector and due to his position, he was able to give cost friendly loan decisions for friends, meaning e.g. longer payment periods. Interviewee 3 put it simple, by saying that "no-one can really be trusted". Possible reasons often seem to come from personal issues, which are never too easily categorised.

5 Data Results and Analysis

To analyse the data, collected from the questionnaire and interviews, this chapter will discuss the findings related to the three investigative questions. The purpose of this analysis is to compare the theory behind internal control with the actual reality and practical processes companies' use. By doing this, some possible failure points might be detected, from where suggestions on how to prevent fraud should arise. The suggestions and possible development ideas will be represented in the final part of this chapter.

5.1 Managers' views on internal control

To tackle the research problem, the first investigative question that needed to be answered was to find out what are managers' views on internal control in general and in their company. Starting the analysis already from the questionnaire answers, it seems as managers in consulting companies have a good or excellent knowledge in internal control. Interpreting the answers concerning the objectives of internal control, all of the respondents had quite a thorough answer to present, giving an impression that the objectives definitely are something, which are discussed and considered within the organisations. The managers understand the importance and necessity of the controls, as said by Interviewee 1 the internal control system ensures that the company objectives are reached. Therefore it can be said that having an internal control system seems to be a natural part, and somewhat a necessity, of the organisations' operations. The topic on objective will still be discussed in more detail in the following chapter, as objective setting is also one of the key components when building an effective internal control system.

According to a definition represented by Glader, a consultant from BDO Oy, internal control should provide added value to the organisation and improve its operations (24 Apr 2012). All of the survey respondents confirmed that their companies' internal control does this. In more precise, according to what was answered, the controls make it possible to provide high-quality service globally, set standard operating principles and ways of working according to policies and guidelines, which brings efficiency, and

keeps employees sharp with internal activities. In addition, the different control activities make accurate, relevant and timely reporting possible. However, as brought up by the interviewees, the extent of the control system should suit the organisational culture and be in proportion with the size of the company. For example, the use of the US SOX reporting system would be too strict for Finland. Interviewee 2 also explained how a too hierarchical system often slows down the processes, and how too intense micromanagement could also be unbeneficial for a company. The best solutions for companies would be to find a golden mean where the amount of control procedures would still create added value and improve the performance of the company.

5.2 Effectiveness of an internal control system

The second investigative question was to find out how effectively an internal control system prevents fraud. To analyse this, the cube presented by COSO is an appropriate tool that can be used (figure 5). As mentioned in chapter 2.5.1, the eight pillars of the cube need to be present and functioning in order for a company to have effective enterprise risk management, including an effective internal control system.

5.2.1 Analysis according to the eight pillars of COSO

Starting from the first pillar, or component, the internal environment of the organisation needs to be in place, as it sets the tone of the organisation, and is the basis for how risks are viewed and addressed by the employees. In the researched auditing companies the tone and the internal environment seem to be in place. The two interviewees from the auditing companies discussed in detail the depth of the knowledge the employees need to have on the policies of the company and the ethical issues providing the philosophy for the businesses. As explained by Interviewee 2, employees are annually tested on their knowledge of the global organisational requirements. Employees seem to understand the importance on what is done and why it is done. By having the company's policies and philosophy as a written text, the company prevents its employees from misinterpreting facts (KPMG 1999, 26).

The internal environment in Interviewee 3's company still seems to need improvements. The tone that comes from the management and upper level supervisors is clearly something affecting the whole internal environment, which currently is not as open as it could be. As referred by Interviewee 3, the blaming culture is something that needs to be overcome, in order to open up the atmosphere. By doing this, meaning making the environment more open, possible risks will be easier to detect and the overall control processes could be better developed and improved. Now, as the communication channels seem to be experiencing blockages, the risk management board might be lacking crucial information, which as a result slows down the flow of continuous development. The phenomenon of a blaming organisational culture can be detected from one of the most common weaknesses in organisations represented by the KPMG's Risk Management Diagnostic (chapter 2.5.2). The aspect of behaviour fails, when disincentives exist which lead employees to behave in a non-functional manner (KPMG 1999, 26). Moreover, the philosophy and setting an example should come from the board, management and supervisors.

Objective setting is the next of the eight components represented in the COSO cube. Through the objectives management is able to identify potential events affecting the company's achievements. The chosen objectives should support and be in align with the entity's mission and be consistent with its risk appetite. The auditing companies' objectives came relatively clear from the survey, where the objectives of the internal control systems are aimed to support the objectives of the organisation. Most of the respondents mention ensuring their brand reputation, managing risks and assuring quality in the work that they provide. Everything an organisation does should have a meaning and clear objectives, which provide the path for reaching goals. According to the research, the respondents were well aware of this.

The third pillar of the COSO cube represents event identification: internal and external events affecting achievements of objectives need to be identified, and determined as risks and opportunities. All of the survey respondents were aware of the nature and extend of the risks facing their organisation, however during the interviews the topic was discussed in more detail. The representatives from the auditing companies were

clearly able to categorise the risks into internal and external. As discussed in chapter 4.2.1 the risks vary from economic downturn to employee know-how. Interviewee 3 categorised their risks under operative, reputation and strategic risks. The operational risks can further be divided into external and internal. The external risks include market risks, credit risks and liquidity risks, which can arise from client and counter party relations. The internal risks were more discussed in relation to the internal control, which moreover include in-house procedures and processes. In all off these researched company cases, it seems that the risks are well known. However, as discussed with Interviewee 3 (chapter 4.2.3) the topic of fraud and controls came more explicit after the misappropriation of assets - incident, which their department experienced. This incident lead to tightening of the controls, but it seems that the atmosphere of openness should still be improved, in order to develop the procedures to be more efficient. Theoretically this can be again assessed as one of the weaknesses under performance and risk effectiveness, where the board does not receive the right information (chapter 2.5.2) (KPMG 1999, 26).

The next two components represented by COSO, risk assessment and risk response, were not discussed in such detail. The risk assessment includes the analysis of the likelihood and impact of risks, in order to determine how the risks should be managed. The risk response should cover how the company should respond to the risks: avoid, accept, reduce or share. As an overall picture, according to all of the interviews, it would seem that in most cases the companies' response for risks is to avoid or reduce, this especially can be seen by the implementation of control procedures. Risks that are accepted may arise from the economic environment. As said by Interviewee 1, these risks are not only downsides but can also create opportunities.

The sixth pillar represents the control activities, which are to ensure that risk responses are effectively carried out, and procedures and policies are set out. The different procedures of internal control were discussed in the three interviews (chapter 4.2.2). The procedures for the auditing companies more or less include regulations related to the client engagements. The policies are set out by centralised instructions and guidelines on reputation, quality and risk management, wherein according to

Interviewee 2's case, ethical and independence issues are of most importance. The procedures represented by Interviewee 3 mainly include the avoidance of dangerous working combinations. In practice this has been implemented for example in the IT programs, by having personal user ID's, with personal settings for different employees. On top of what have been mentioned, the internal audits are also considered as a form of implemented procedures. However, according to the COSO cube, these could be categorised under the final pillar of monitoring as well. But as it was mentioned, all of the components are interrelated, and some topics can be discussed under more than one of the pillars.

The second last of the pillars represents information and communication. Relevant information needs to be identified, captured, and communicated in a manner that employees can carry out their responsibilities. Effective communication is as well flowing down, across, and up the organisation. (COSO 2004, 5.) The information flow and communication regarding internal control policies and philosophy were discussed with the interviewees. More or less in all of the three companies, which were represented by the interviewees, the communication on these topics mainly happens through regulations, learning material and different publications (chapter 4.2.2). Interviewee 1 refers to their quality risk management training material. Interviewee 2 explains about their annual web-based surveys and compulsory e-learning on ethical issues. Interviewee 3 discusses about an annually published risk management plan, and additional risk management education for the supervisors. As an overall interpretation of the situation, it seems there are no lacks in information flow from the top to bottom, however based on these answers it is hard to say about the communication flowing across and up.

The final pillar represents monitoring: the entire risk management needs to be monitored, and necessary modifications should be made when needed. The monitoring happens through management activities and separate evaluations. The aspect of monitoring was discussed with the three interviewees (chapter 4.2.2). In Interviewee 1's case the monitoring happens from their group's India office. They follow the procedures especially related to client and engagement acceptances that have been

carried out. In addition they follow the revenue generation within the period of a specific project. Interviewee 2 also refers to the external monitoring executed by the global company group. In more precise, the internal audits are one mean of monitoring the operations of the Helsinki office. The two auditing companies are also required to report on their risk management on a regular basis. Interviewee 3 explains how the risk management board and the external auditors (in this case the representatives of the Big Four) act as the monitoring organs. In addition to these, the company is required to report on risk management issues to the board as well as the Finnish Financial Supervisory Authority. According to the description of monitoring published by COSO, it seems that all of these companies' operations are adequately monitored. However, the concept of remote monitoring from a different continent raises a few questions; can the reliability of the network systems be trusted? And even though the big picture can be monitored in such, how about the details related to daily processes? Even though, the auditing companies and their employees do have requirements on reporting locally, the objectivity of the monitoring can be speculated.

5.2.2 Findings according to the eight pillars of COSO

As a conclusion of the effectiveness of the current internal control systems, which have been examined in the previous chapter, Table 3 presents an overall generalisation of the situation. The table looks at the systems by assessing the presence and functionality of the eight components compromised in the COSO cube. The final column provides considerations on what can be improved by companies, when considering each of the components separately.

Table 3. Overview of the internal control systems efficiency

THE EIGHT PILLARS	CURRENTLY	CONSIDERATION
Internal Environment	Mostly functioning, but improvements needed.	• Open communication channels • Learning from mistakes, rather than blaming culture – aspect of behaviour
Objective Setting	Present and functioning.	• Consistency with risk appetite and mission
Event Identification	Mostly functioning, but improvements needed.	• Improvements for performance and risk effectiveness – lack of relevant communication to the board • → not all possible risks are detected
Risk Assessment	N/A	• Deeper analysis on likelihood and impact of risks
Risk Response	Present and functioning.	• When to avoid, accept, reduce or share risks? • Cost of control vs. benefit
Control Activities	Present and functioning.	• Careful consideration of all internal risks • Balance between too intense controls and what is necessary – e.g. proportion with the company size
Information and Communication	Mostly functioning, but improvements needed.	• Information flow should go across, up and down
Monitoring	Mostly functioning, but open for interpretation.	• Importance of local monitoring?

However, as mentioned in chapter 2.5.1, the eight components do not function identically in all organisations. In smaller organisations they may be less structured and more informal, but still effective. According to the analysis presented in the previous chapter, it seems as if the consulting companies set an example to other companies. The theoretical components required for an effective system of internal controls seemed more or less to be in place. The company, represented by Interviewee 3, on the

other hand would need improvements to its internal environment, and possibly to its control procedures. Positively it can be seen that the topic of implementing, developing and updating internal control systems is currently discussed in many organisations.

To answer how effectively do the internal control systems prevent fraud, we can reflect on what was answered in the surveys and what other conclusions can be made based on the presented data. As suggested in chapter 4.1.2, internal control plays a high role in preventing fraud however it cannot fully prevent it. Already COSO describes the limitations of the ERM, which arise from human mistakes and errors. These of course are a natural part of operations that are run by people, and therefore something that is impossible to totally prevent. However, fraud is something considered and done intentionally, and should not be interpreted to be the same as mistakes or errors. Nevertheless, the limitations might refer to the mistakes done with the implementation of the internal control system, which could then create opportunities for fraudulent behaviour. If interpreting this as such, then one could say that an effective internal control system would indeed prevent fraud.

5.3 Prevention of fraud

The third and final investigative question was how to prevent fraud in the very initial stages, and what are the development ideas and suggestions to improve internal control? To tackle the first part of the question (how to prevent fraud), the initial approach could be to view the situation by using the Fraud Triangle model (chapter 2.1). According to the theory behind the Fraud Triangle, all of three components of opportunity, motivation and rationalisation, need to be in place for fraud to happen (Harrison et al. 2011, 234; Ernst & Young 2009, 1). From these three factors, motivation and opportunity are something the organisation can have an effect on. When thinking about the very initial stages, even before implementing internal controls in order to prevent opportunities, the actual crucial factor is the motivation. Ernst & Young refers to the motivation by a different term: pressure (2009, 1). The pressure can be created by a demand for higher earnings, or it can be something arising from

the top of the company. One way or another, it is something that is the underlying reason for the fraud act.

As discussed with the interviewees, the main reasons for fraud do not seem to be the existing opportunities, but something that motivates a person to commit the fraud. For example, in the case presented by Interviewee 3 (chapter 4.2.3), the employee had worked in the same company for 30 years, and it is assumable that the same opportunity had existed throughout the years. However, it seems that during the past year something had happened in the employee's personal life that created the pressure and motivation, pushing the employee to act and to commit fraud. At this point the appropriate controls should have been in place. However, one could argue on would it have made a difference. In this case most probably yes, the asset misappropriation would have been more difficult to conduct. But in cases where a person has been pressured to its limits, the person would probably find its opportunity, in one way or another. Nevertheless, in today's corporate world, an organisation should be able to have an effect on its employees' motivation. Interviewee 1 presented an interesting example on how to have an effect on the employees' motivation. Their organisation has included the compliancy with the quality and risk management as a part of their remuneration program. If corners are cut, the employee doesn't receive a bonus. Other examples of effecting the employee motivation fall under human resource management. Continuous or regular discussions on job satisfaction, and for example salary discussions, should definitely be in place. By doing this, the company reduces on behalf of itself the risk of providing the motivation for its employees. With creating a balance of effective controls and supporting working environment, a company can minimise fraudulent behaviour.

For what it comes to development ideas and future suggestions, it seems the theories related to internal control and risk management can provide a few. To pinpoint some of the components, which seem to need improvements in the researched examples, especially by Interviewee 3's company, we can take a look at Table 3, representing the overview of the internal control systems efficiency. The components, which explicitly need more consideration include the internal environment, event identification,

information and communication, and possibly monitoring. When analysing the data represented by the interviewees, it becomes apparent how interrelated the different components are in practice. In all of the cases it seems the internal environment sets the base, as well as the limitations to event identification, and information and communication (figure 9).

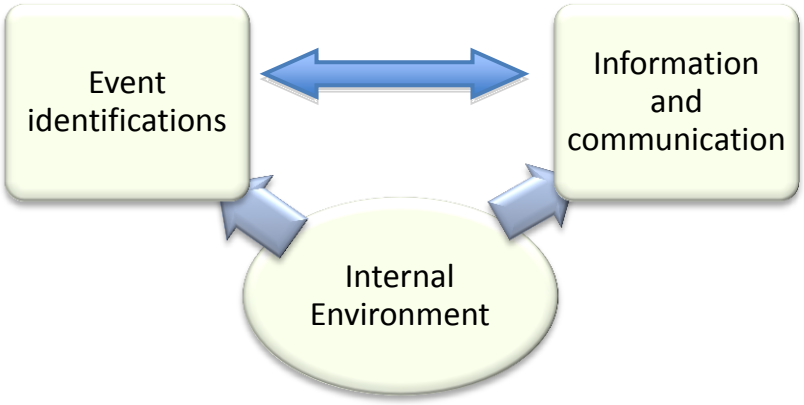

Figure 9. Interrelation of components

To take as an example the company case presented by Interviewee 3, it could be concluded that the information and communication as well as the event identification components would function better if the internal environment would be more open, and have a more accessible atmosphere. With an open and functioning internal environment, the information flow would become more efficient, and the communication channels could operate in all necessary directions. The component of event identification would function better, as if the communication channels were open, the information would flow fluently. Therefore help the board to identify events, which affect the achievements of objectives, and determine these events as risks and opportunities.

The component of monitoring seems to be an aspect possibly also in need of deeper consideration. Even though, the research findings do not suggest that there are any negative aspects in monitoring happening across borders, companies should definitely consider the effectiveness and reliability of distant monitoring. Nowadays, as the world is full of international organisations operating in multiple continents, a level of monitoring happening across borders is inevitable. Therefore, companies should

carefully consider the implementation of internal control, and determine the organ that is ultimately in charge of implementing and carrying-out the processes of their internal control system. In addition to what the headquarters, or the parent company monitors, local monitoring of control procedures is in place.

6 Conclusions

Fraud and deception seem to be overall something that a willing and determined person will find a way to commit. Therefore, it is not valid to say that a corporate internal control system would prevent fraud. Nevertheless, internal control is something that minimizes the opportunity and in such it is a necessity for all companies to have. This final chapter presents the validity and usefulness of the discussed results, possible recommendations for future research, and finally the researcher's personal experience on professional development and learning during the thesis process.

6.1 Validity and usefulness of results

The validity of the research can be examined through the existing data on earlier research (chapters 2.2 and 2.4), done by COSO and Ernst & Young, and the data received from the survey respondents and the interviewees. There are two valid conclusions that can for sure be made based on the research. Firstly that financial fraud exists and it can affect companies of all size; and secondly that internal control should be a natural part of every company's risk management. The results and analysis chapter is based on the answers received from the survey as well as the interviews. As the respondents (excluding Interviewee 3) have been from the highly respected Big Four auditing companies, there is no reason to doubt the reliability of the answers. However, of course as the received answers are in a relatively small scale, no greater generalisations can be made. Instead the answers and results should be interpreted as opinions of the field's experts.

The usefulness of the research can be observed for example, first of all from the Interviewee 3's point of view. The thesis provides a few useful considerations for the company, as presented in chapter 5.2.2; there definitely is a need for improvements in creating a more functioning internal environment, which would positively affect the information and communication flow as well as the event identification processes.

Further research on the topic could include investigating the co-operation between managers, the board and the external auditors. As can be seen in the cases of Enron and the Lehman Brothers, the external auditors were present, but still they did not detect the fraudulent reporting, or if they did, they did not act on it. Even though the employee level procedures seem to be highly emphasised in the theoretical models of internal control, could or should there be something similar provided for the top of the company?

The research also provides new and interesting learning for fellow students and educators. Linking ethical issues with finance brings out important factors, which too often are left out of the curriculum. The topic of financial fraud is not easy to tackle, but creating awareness of the consequences and the seriousness of it, can in the long run reduce fraud incidents, and maybe even create a more trustworthy business society. Corporate social responsibility and ethical business behaviour are something expected from all HAAGA-HELIA international business graduates. This thesis provides good insights in regarding to the mentioned, especially for students specialising in finance.

6.2 Own professional development and learning

During the thesis process I have learned a multiple different things. The whole process has taken a bit over a year, and for me this has been the longest period of time I have ever focused on writing one piece of text. Merely this has required patience and a lot of thinking through. During the whole process, the most difficult thing has been to stick with the demarcated topic. For example every time I have written something I have had to remind myself not to go too far, despite interesting findings and facts. But, I am grateful I started researching this topic, as throughout the process I have kept my motivation, and I am also glad that I can actually present some findings on it.

Some setbacks that I experienced happened firstly with the Webropol - survey, as I had some minor technical difficulties with it, and therefore probably lost a few of the respondents' answers. In total I sent the survey five times, however only six out of 19 people replied. Successfully, the interviews compensated this, and I was able to get

interesting answers. The highest learning probably happened with contacting the different companies and conducting the interviews.

References

Aaltola, J. & Valli, R. 2001. Ikkunoita tutkimusmetodeihin II. Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. PS-kustanus. Jyväskylä.

Beasley, M., Carcello, J., Hermanson, D. & Neal, T. 2010. Fraudulent Financial Reporting: 1998-2007. An Analysis on U.S. Public Companies. URL: http://www.coso.org/documents/COSOFRAUDSTUDY2010_001.pdf. Accessed: 23 Jul 2012.

Bloomberg BusinessWeek 2009. The Meltdown: One year later. URL: http://www.businessweek.com/investing/special_reports/20090910the_meltdown_one_year_later.htm. Accessed: 29 Jan 2012.

Collier, P., Berry, A. & Burke, G. 2007. Risk and Management Accounting. Best practice guidelines for enterprise-wide internal control procedures. 1st ed. CIMA Publishing. Oxford.

COSO 2011. URL: http://www.coso.org/guidance.htm. Accessed: 22 Jan 2012.

COSO 2004. Enterprise Risk Management – Integrated Framework. Executive Summary. URL: http://www.coso.org/documents/coso_erm_executivesummary.pdf. Accessed: 5 Jun 2012.

Ernst & Young 2009. Detecting financial statement fraud. What every manager needs to know. URL: http://www.ey.com/Publication/vwLUAssets/FIDS-FI_DetectingFinancialStatementFraud.pdf/$FILE/FIDS-FI_DetectingFinancialStatementFraud.pdf. pp.1-4. Accessed: 23 Feb 2012.

Financial Times Lexicon 2012. URL: http://lexicon.ft.com/Term?term=big-four. Accessed: 22 Oct 2012.

Freifeld, K. & Sandler, L. 22 December 2010. Bloomberg News. Cuomo Sues Ernst & Young for Assisting Lehman Brothers in `Repo 105' Fraud. URL: http://www.bloomberg.com/news/2010-12-21/new-york-s-cuomo-said-to-plan-fraud-suit-against-lehman-s-accounting-firm.html. Accessed: 29 Jan 2012.

Glader, H. 24 Apr 2012. Sisäisen Tarkastuksen Arviointiprosessi. Consultant. BDO Oy. HAAGA-HELIA University of Applied Sciences' seminar presentation. Helsinki.

HAAGA-HELIA 2012a. Degree Program in International Business, Helsinki Pasila Campus. URL: http://www.haaga-helia.fi/en/education-and-application/bachelor-degree-programmes/business/degree-programme-in-international-business-pasila-campus-youth/index_html. Accessed: 24 Oct 2012.

HAAGA-HELIA 2012b. About HAAGA-HELIA. URL: http://www.haaga-helia.fi/en/about-haaga-helia/haaga-helia-in-a-nutshell. Accessed: 8 Nov 2012.

Harrison, W., Horngern, C., Thomas, C. & Suwardy, T. 2011. Financial Accounting. International Financial Reporting Standards. 8th ed. Pearson Education South Asia. Singapore.

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu. Teemahaastattelun historia ja käytäntö. Gaudeamus. Helsinki.

IIA 2004. The Institute of Internal Audits. Applying COSO's Enterprise Risk Management – Integrated Framework. PowerPoint presentation. September 29, 2004. pp.7-8. Accessed: 5 June 2012.

KPMG 1999. The KPMG Review. Internal Control: A Practical Guide. URL: http://www.ecgi.org/codes/documents/kpmg_internal_control_practical_guide.pdf. Accessed: 27 Mar 2012.

Palepu, K. & Healy, P. 2003. Negotiation, Organizations and Markets Research Papers. Harvard NOM Research Paper No. 03-38. The Fall of Enron. pp. 3-19. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=417840. Accessed: 4 Jul 2012.

Roger, S. 2010. The History of unethical accounting behavior. URL: http://www.ehow.com/facts_7468853_history-unethical-accounting-behavior.html#ixzz1kYROge9W. Accessed: 4 Nov 2011.

Sarbanese-Oxley Act 2002. Sarbanes-Oxley Act Section 404. URL: http://www.soxlaw.com/s404.htm. Accessed: 26 Jul 2012.

The NewYork Times 2012. Lehman Brothers Holdings Inc. URL: http://topics.nytimes.com/top/news/business/companies/lehman_brothers_holdings_inc/index.html. Accessed: 12 Jul 2012.

UCMerced 2012. Controls and Accountability. The Fraud Triangle. URL: http://controls.ucmerced.edu/fraud-triangle.aspx. Accessed: 22 Feb 2012.

United States Securities and Exchange Commission 2008. Quarterly Report. Lehman Brothers Holdings Inc. URL: http://www.rns-pdf.londonstockexchange.com/rns/8436Z_1-2008-7-24.pdf. Accessed: 24 Oct 2012.

Wikipedia 2012. Accounting Scandals. URL: http://en.wikipedia.org/wiki/Accounting_scandals. Accessed: 29 Jan 2012.

Attachments

Attachment 1. Overlay matrix

Research Problem How to prevent accountants and managers from conducting financial fraud – importance of an internal control system?		
Investigative Questions (IQs)	**Theoretical Framework (concepts & models)**	**Results**
IQ1: What are the management's views on internal control generally and in their company? Example of real practice: current internal control system.	• Fraud Triangle • Internal control	• All companies should have. • Necessary part of risk management. • Implementation according to corporate culture and company size. (chapter 5.1)
IQ2: How efficiently does an internal control system prevent fraud?	• Fraud Triangle • Internal control • COSO ERM • COSO cube • Risk Management Diagnostic (by KPMG)	• If properly implemented, the internal controls prevent fraud: factors related to opportunity and motivation. (chapter 5.2)
IQ3: How to prevent fraud in the very initial stages? What are the development ideas and suggestions to improve internal control?	• COSO cube • Internal control • Fraud Triangle	• Implementing an open internal environment with a functioning and efficient internal control system. (chapter 5.3)

Background

1. Please, state your position in the organisation?

2. How many years of work experience do you have on this field?

- 0-1 years
- 1-3 years
- 3-5 years
- 5-10 years
- 10 or more years

3. What is your knowledge on Internal Control? (From scale 1 to 5, where 1= poor, 5= excellent) *

	1	2	3	4	5
Internal Control	◉	○	○	○	○

Internal control

Decision making, roles and responsibilities

4. From 1-5 how aware are you of your own role and responsibilities in the organisation (1= not at all, 5= very aware)?

	1	2	3	4	5
Role & responsibilities	○	○	○	○	○

5. How often do your responsibilities require only your decision making? (1= rarely, 3=sometimes, 5=daily)?

	1	2	3	4	5
Decision making	○	○	○	○	○

6. Are responsibilities written to the employees' job descriptions?

<-- Edellinen Seuraava -->

Internal control

Controlling the company (current IC system)

7. When was your company's internal control system first implemented?

8. What are the objectives of your company's internal control system?

9. Who (in what position) is/are in charge of the company's risk management?

10. Who (in what position) is/are in charge of the company's internal control?

11. Are you aware of the nature and extend of the risks facing your organisation?

- yes
- no
- maybe

12. Is your organisations internal controller an employee from the organisations payroll or hired outside the organisation?

13. If hired internally, how is the objectivity of the controller verified?

14. How often does your company have internal audits?

- Annually
- Every second year
- Other

15. What are the consequences, if risks are detected during an internal audit?

16. Does your organisations current internal control system improve your organisation's performance? If yes, how? If no, how?

Yes No

17. How effectively does your company's internal control system prevent fraud? (1= not at all, 3= moderately, 5=highly)?

	1	2	3	4	5
Preventing fraud					

18. Are there opportunities for employees to conduct fraud? (1= not at all, 3= moderately, 5=highly)?

	1	2	3	4	5
Opportunities for fraud					

19. Are there opportunities for managers to conduct fraud? (1= not at all, 3= moderately, 5=highly)?

	1	2	3	4	5
Opportunities for fraud					

Internal control

Board meetings

20. How often are the risk management and risk analysis reviewed by the board?

- Quarterly
- Annually
- Every second year
- Other
- I'm not aware

21. How often is the internal control system reviewed by the board?

- Quarterly
- Annually
- Every second year
- Other
- I'm not aware

<-- Edellinen Seuraava -->

Internal control

Relationships

22. How transparent are the relationships with stakeholders? (1= not at all, 3= moderately, 5=highly)?

	1	2	3	4	5
Transparency	○	○	○	○	○

23. How are relationships between clients and other stakeholders controlled?

24. After an employee resigns, what kind of regulations do you have for confidential information?

<-- Edellinen Seuraava -->

Fraud

25. In your organisations history, have there been cases related to fraud?

- ○ Yes
- ○ No
- ○ Maybe

26. If yes, under which category have they been related to:

- ☐ Misappropriation of assets
- ☐ Fraudulent financial reporting
- ☐ Corruption (e.g. conflict of interest, bribery, extortion)
- ☐ Other

27. What have been the consequences and how has the situation been handled?

28. What have been the main reasons for fraud?

29. Any final comments on the topic:

<-- Edellinen Lähetä

Attachment 3. Interview Framework

Background

1. What is your position in the organisation? –could you give a brief description of your daily tasks?

2. How many years of work experience do you have on this field? In this organisation?

Controlling the company (current IC system)

1. What components does your risk management include?

2. Internal control can be defined as "a system of procedures implemented by company management" (Harrison et. al. 2011, 237.) What kind of procedures would you say your internal control includes?

3. Are you aware of the risks facing your organisation? Can you give an example of a risk?

4. How are your company's internal audits usually conducted?
   - How often, and what are some basic elements?

5. Do you think your internal control system could be improved? –Have you detected any possible failure points?

6. In practice, how is the internal control system (or/and enterprise risk management) monitored?

Responsibilities, Philosophy and Policy

1. Is your company obliged to report on internal control? (E.g. as in the US Sarbanes-Oxley Act)
   - How often and to what extend?

2. Are your internal control policies and philosophy defined on paper and communicated throughout the organisation? (E.g. From the top of the company – basis for how risk is viewed and addressed by the employees.)
- By email/meetings/intranet/other?

3. Can you describe your organisations culture and what is the general view on internal control among the employees?

Fraud

1. During your carrier in this field, have you come across on cases related to fraud?

- If yes, under which category have they been related to:

  -misappropriation of assets
  -fraudulent financial reporting
  -corruption (e.g. conflict of interest, bribery, extortion)
  -other

- What have been the consequences and how has the situation been handled?

2. What would you say are the main reasons for fraud?

3. Do you think there is a need for an internal control system for every company?
   - are there any negative factors of having an internal control system?

Final comments on the topic?