UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

A FRAUD AUDITING APPROACH FOR THE REGULATOR TO DETECT INVESTMENT FRAUD SCHEMES

By

Wendy Hattingh
Student Number: 91047987

Submitted in partial fulfilment of the requirements for the degree

MPhil in Fraud-Risk Management

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

Department of Accounting

at the

UNIVERSITY OF PRETORIA

Study leader:

Mr D du Plessis

2011

DEDIDICATION

I am dedicating this dissertation to my daughter Vianca. Thank you for your understanding and sacrifices through this process.

Special thanks also to my husband Arend for your love and encouragement, my parents Tonie and Ria Drotsky for always being there when I needed you and my study leader Danie du Plessis for all your input. The writing of this dissertation was difficult at times but with the grace of the Heavenly Farther and support from all I was able to have the privilege to develop.

ABSTRACT

Investment managers are entrusted with clients assets and should act with due care and diligence when dealing with it. The regulation of investment managers does not preclude the possibility that they can defraud their clients. The question posed by this research is whether the regulator can as part of its risk-based supervision methodology apply a fraud auditing approach to identify possible investment fraud schemes. The regulatory mandate and powers to pro-actively detect fraud is considered as well as the changes required to the regulator's methodologies.

Keywords:
Financial statement fraud
Fraud auditing
Investment fraud schemes
Investment manager
Red flags
Regulator
Risk-based supervision onsite visits

TABLE OF CONTENTS

GLOSSARY OF TERMS 1

CHAPTER 1: INTRODUCTION 4

1.1 INTRODUCTION 4
1.1.1 Investment fraud by investment managers 4
1.1.2 The role of the external auditors versus the role of the regulator in detecting fraud 5
1.1.3 A regulatory approach to the supervision of investment managers 6
1.1.4 A fraud auditing approach 8
1.1.5 Fraud auditing techniques that can be used in regulatory supervision 9
1.2 THE RESEARCH PROBLEM 9
1.3 PURPOSE STATEMENT 10
1.4 RESEARCH OBJECTIVES AND QUESTIONS 10
1.4.1 Primary objective 10
1.4.2 Secondary objectives 10
1.5 IMPORTANCE AND BENEFIT OF THE PROPOSED STUDY 11
1.6 RESEARCH METHODOLOGY 11
1.7 DELIMITATIONS AND ASSUMPTIONS 14
1.8 CHAPTER OUTLINE 15
1.8.1 Chapter 2: Defining investment fraud schemes 15
1.8.2 Chapter 3: The supervision of investment managers and risk-based onsite visits 15
1.8.3 Chapter 4: The use of a fraud auditing approach 16
1.8.4 Chapter 5: The applicability of a fraud auditing approach in detecting investment fraud schemes 16
1.8.5 Chapter 6: Conclusion: on the use of a fraud auditing approach in detecting investment fraud 16

CHAPTER 2: DEFINING INVESTMENT FRAUD SCHEMES 17

2.1 INTRODUCTION 17
2.2 DEFINING FRAUD 17
2.2.1 White-collar crime 17
2.2.2 Definitions and elements of fraud 18
2.2.3 Classifying the different types of fraud 20
2.3 FRAUD COMMITTED BY PERSONS IN POSITIONS OF TRUST 21
2.4 SPECIFIC EXAMPLES OF INTERNATIONAL INVESTMENT FRAUD SCHEMES 23
2.4.1 The South Sea Bubble 23
2.4.2 Charles Ponzi 24
2.4.3 Investors Overseas Services (“IOS”) 26
2.4.4 Hedge fund investment fraud 27

2.5 INVESTMENT FRAUD SCHEMES IN THE SOUTH AFRICAN FINANCIAL SERVICES INDUSTRY 29
2.5.1 Common Cents Investment Portfolio Strategists and Ovation Global Investment Services 29
2.5.2 Fidentia Holdings 30
2.6 CONCLUSION 32
CHAPTER 3: THE SUPERVISION OF INVESTMENT MANAGERS 34
3.1 INTRODUCTION 34
3.2 MARKET CONDUCT REGULATION 35
3.3 THE SUPERVISION OF INVESTMENT MANAGERS 38
3.4 REGULATORY ONSITE VISITS 40
3.4.1 The risk-based supervision approach of FSA 40
3.4.2 Examinations by the SEC's Office of Compliance Inspections and Examinations (OCIE) 42
3.4.3 FSB's Onsite visits to investment managers in terms of the FAIS Act 44
3.5 CONCLUSION 46
CHAPTER 4: THE USE OF A FRAUD AUDITING APPROACH 48
4.1 INTRODUCTION 48
4.2 COPORATE GOVERNANCE STRUCTURES APPLICABLE TO THE PREVENTION AND DETECTION OF FRAUD 49
4.3 WHAT DRIVES PEOPLE TO COMMIT FRAUD? 51
4.4 FRAUD AUDITING 52
4.5 THE DIFFERENCE BETWEEN FRAUD AUDITING AND FRAUD INVESTIGATION 53
4.6 THE FRAUD AUDITING APPROACH 54
4.6.1 Identifying the intrinsically fraudulent scheme and any of its variations 55
4.6.2 Fraud opportunities 56
4.6.3 The fraud scenario 57
4.6.4 Building a data profile of the fraud scheme 58
4.6.5 Data mining to search for transaction data profile 58
4.6.6 Fraud auditing procedures 59
4.6.7 Considering the evidence 60
4.6.8 Reaching a conclusion on the evidence of possible fraud 61
4.7 CONCLUSION 61
CHAPTER 5: THE APPLICABILITY OF A FRAUD AUDITING APPROACH TO DETECT INVESTMENT FRAUD SCHEMES 63
5.1 INTRODUCTION 63
5.2 FRAUD AUDITING PROCEDURES USED TO DETECT MANAGEMENT FRAUD 64
5.3 BRAINSTORMING 64

5.4 ANALYTICAL PROCEDURES USED IN THE DETECTION OF FRAUD 65
5.4.1 Financial statement analysis 66
5.4.2 Reasonableness testing 69
5.4.3 Data-mining analysis 70
5.5 THE USE OF INTERVIEWS TO DETECT FRAUD 70
5.6 OTHER METHODS USED TO DETECT MANAGEMENT FRAUD 71
5.7 RED FLAGS IN MANAGEMENT FRAUD 72
5.7.1 Aggressiveness of executive management and limitations in corporate governance structures 73
5.7.2 Internal control weaknesses 74
5.7.3 Unexpected or unusual financial performance 74
5.8 TARGET FRAUD RISK ASSESMENT 75
5.9 THE USE OF A FRAUD AUDITING APPROACH IN DETECTING INVESTMENT FRAUD SCHEMES 76
5.10 CONCLUSION 78
CHAPTER 6: CONCLUSIONS ON THE USE OF A FRAUD AUDITING APPROACH TO DETECT INVESTMENT FRAUD 80
6.1 SUMMARY OF FINDINGS AND CONCLUSION 80
6.1.1 Investment fraud and its similarities to management fraud 80
6.1.2 The regulator's role in detecting investment fraud 81
6.1.3 The applicability of a fraud auditing approach to enhance regulatory onsite visits 83
6.2 RECOMMENDATIONS 86
6.3 CONTRIBUTION OF THE STUDY AND FURTHER RESEARCH 87
REFERENCES 88

GLOSSARY OF TERMS

Client, consumer and investor

A client is a specific person who entrust the management of its investment to an investment manager (Millard & Hattingh 2010, p.12). Client, consumer and investor will be used interchangeably in this study.

Financial Services Board ("FSB")

The FSB was established in terms of the Financial Services Board Act (96/1990). The FSB is referred to as the regulator of financial institutions. The provisions of the FSB Act (96/1990) established the FSB as a creature of statute. The FSB functions outside the public service although the Minister of Finance appoints its board members and its executive officer. The function of the FSB is to supervise financial institutions that are licensed or authorised by various acts of parliament, such as investment managers that are licensed in terms of the Financial Advisory and Intermediary Services ("FAIS") Act (37/2002). The objective of the FAIS Act (37/2002) is to protect consumers and ensure that investment managers act with due care and diligence when dealing with clients' funds.

Fraud auditing

It is not the sole purpose of an audit to detect management fraud (Vona 2008, p.20). Vona (2008, p.27) states that the goal of fraud auditing is *"to offer an opinion regarding the existence of fraud*". Fraud auditing can, therefore, be described as the application of auditing procedures to a sample of transactions to identify any possible fraud (Vona 2008, p.27). There do not need to be any allegations of fraud or an internal control weakness that indicates the existence of fraud – for fraud auditing to be performed (Singleton, Singleton, Bologna, Lindquist 2006, p.55). Fraud auditing is a proactive approach to search for the existence of fraud (Vona 2008, p.19).

Financial statements

Financial statements reflect the financial position of an entity (balance sheet), the results of its operations (income statement), cash flow position (cash flow statement), change in equity and significant accounting policies and explanatory notes to the above (FAIS Act 37/2002, sec.19).

Financial statement fraud and management fraud

Financial statement fraud involves the purposeful misstatement or omission of amounts, or failure to disclose, financial information from the financial statements – in order to deceive the users of financial statements – in particular, investors and creditors (Wells 2008, p.299). Financial statement fraud includes false, altered or manipulated financial records, documentation or business transactions, deliberate material omissions or misrepresentations of transactions, misapplication of accounting policies and procedures and intentional omission of disclosures (Wells 2008, p.299). Financial statement fraud is also referred to as management fraud (Albrecht *et al*. 2009, p.355). Financial statement fraud and management fraud are used interchangeably in this study, as management is held responsible for the fair presentation, integrity and quality of all financial statements (Rezaee & Riley 2010, p.5).

Investment fraud schemes

For the purpose of this study investment fraud schemes is defined as the intentional misrepresentation made by investment managers relating to investments entrusted to them by their clients (investors) that causes actual or potential prejudice to the client. These schemes can either originate from the investment manager that has good intentions, but loses money due to bad investment decisions, and then defrauds clients into believing that they are earning a good return on their investments. It can also originate from a fraudster deceiving his/her clients from the start, with the intention of stealing clients' funds, and then defrauding them to believe their investment is earning returns (Coenen 2008; Albrecht 2003; Snyman 2007).

Investment managers

In South Africa, all investment managers must be authorised in terms of the FAIS Act (37/2002), as discretionary financial services providers. Investment managers are organisations that fall within the definition of a financial institution in terms of the FSB Act (96/1990). Investment managers manage financial products (securities, shares, bonds etc.) on behalf of their clients (investors) in terms of an agreed mandate to meet specified investment goals (FAIS Act 37/2002).

Red flags

Different types of fraud exist and each type of fraud has different symptoms that indicate the likelihood of its existence (Rezaee & Riley 2010, p.105). Red flags are indicators or signals that a potential problem exists; and they might be an early warning that fraud symptoms are present. They indicate that there is a potential for fraud schemes (Vona 2008, p.13; Rezaee & Riley 2010, p.86). The symptoms of fraud can be events, conditions, situational pressures, opportunities or personal characteristics that cause a person to commit fraud (Koornhof & Du Plessis 2000, p.72).

Red flags can be categorised as behavioural, transactional, systemic or corporate; and they may be reactive (those noticed by a trained eye) or proactive (those needing the help of a detector) (Iyer & Samociuk 2006, p.77). Red flags need to be investigated further to determine whether there is any explanation for a particular situation, or if fraud exists (Coenen 2008, p.128).

Regulatory onsite visits

With regard to investment managers, regulatory onsite visits are visits performed in terms of section 4 of the FAIS Act (37/2002) to discretionary financial services providers (investment managers) by the employees of the FSB. These visits form part of the FSB's risk-based supervision methodology in supervising investment managers. Onsite visits entail a detailed review of investment managers' business to determine compliance with the FAIS Act (37/2002).

Risk-based supervision methodology

Risk-based supervision is a structured approach that the regulator follows in the processes of licensing and supervising institutions. Whereby, the risk the entity poses to regulatory objectives is identified as soon as possible; it is then prioritized and mitigated. The objective of risk-based supervision is to assess the soundness of regulatory institutions and intervene on a timely basis – where the practices of institutions are deemed irresponsible (Stewart 2005, p.44).

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

1.1.1 Investment fraud by investment managers

Internationally, the focus on the world economic crisis has been highlighted by investment fraud schemes, such as the recent Madoff Ponzi Scheme (Clauss, Rincalli & Weisang 2009). This has made the financial services regulators worldwide rethink their approach to combating fraud committed by regulated entities, such as investment managers (Aquilar 2009).

Investment managers in South Africa are regulated by the FSB, in terms of the FAIS Act (37/2002). There have been several alleged investment fraud schemes construed by regulated investment managers, such as: Fidentia Holdings (Pty) Ltd ("Fidentia") (FSB 2007a; Ghiwala & Papadakis 2009); Common Cents Investment Portfolio Strategists (Pty) Ltd ("Common Cents") (Griffiths 2006); Ovation Global Investment Services (Pty) Ltd ("Ovation") (Peterson & Levin 2007) and Corporate Money Managers (Pty) Ltd ("CMM") (FSB 2009b).

In these cases, the FSB, as in the well-known investment fraud scheme cases of Owen Wiggins (Nel 1999) and Masterbond (Pillay 2008), applied to the High Court to place the entities, and their associates, under curatorship – in terms of the provisions of the Financial Institutions (Protection of Funds) Act (28/2001, sec.5). The purpose of the curatorship applications was to unwind the alleged fraudulent investment schemes, and to recover some of the alleged embezzled funds of the investors (FSB 2006).

In the cases referred to above, investment managers allegedly defrauded investors by making them believe that their investments were secure, while the management allegedly used the funds – either for their own purposes; or they lost it through bad investment decisions. This was hidden from investors, who believed their investments were intact, while still earning income and capital growth for them (Griffiths 2006; Ghiwala & Papadakis 2009; FSB 2009b).

It is not easy to detect investment fraud, especially if there is no clear indication that it exists. This makes it even more difficult for regulators, who are external to the entity, to identify fraudulent investment schemes that investment managers use to defraud their clients (van de Bunt 2010, p.436).

1.1.2 The role of the external auditors versus the role of the regulator in detecting fraud

Investment managers' annual financial statements are subject to auditing requirements, in terms of the FAIS Act (37/2002). The audit does cover off-balance sheet assets held on behalf of clients. The auditors are required, in cases where client's funds are kept in safe custody, to perform additional procedures, and to issue a limited assurance report on the separate account a manager keeps for depositing clients' funds (FAIS Act 37/2002). However, the auditing of investment managers' financial statements and the separate accounts do not necessarily guarantee the discovery of fraud committed in relation to investor funds (International Federation of Accountants ("IFAC") 2010, p.158). Koornhof and Du Plessis (2000, p.71) indicate that the readers of financial statements expect auditors to uncover any fraud.

Fraud detection surveys, such as the Association of Certified Fraud Examiners ("ACFE") report to the Nations (2010, p.5), indicates that respondents view audits as the most effective fraud-detection mechanism. This is, however, not the most effective mechanism for detecting fraud (ACFE 2010, p.16).

However, in the curatorship case of Ovation, the auditor reported a material irregularity, in terms of section 19(4) of the FAIS Act/2002. This led to further investigations by the FSB (FSB 2006). The auditors of Ovation identified irregularities relating to the investments made into Common Cents, during the audit of Ovation's clients' investments. They immediately informed the FSB of possible fraud (Peterson & Levin 2007) . In the case of CMM, it was not the auditors that identified the irregularities relating to clients' funds, but the trustees of the CMM Collective Investment Scheme (Cobbett 2009).

The regulator cannot, therefore, be over-reliant on the detection of fraud by external auditors. They need to adopt alternative supervisory tools to manage the fraud risk that financial institutions pose to the regulator's objectives.

1.1.3 A regulatory approach to the supervision of investment managers

For purposes of this study the supervision approaches of the United States of America ("USA") and the United Kingdom ("UK") will be discussed and compared with the South African approach. Although the UK's and USA's regulatory approaches differ from each other, it is regarded as setting best international practices in regulation (Fresh & Baily 2009, p.2).

Cendrowski, Martin and Petro (2007, p.16) state that policy makers are using laws, regulations and internal control systems along with traditional coercive methods. In the USA, several agencies such as the Securities Exchange Commission ("SEC") were established not only to detect fraudulent behaviour but also to deter fraud. The SEC was formed after the 1929 stock market crash with the purpose to administer several pieces of legislation relating to the sale of securities, including the USA Investment Advisers Act of 1940 that regulates investment advisors (managers) (Cendrowski et al. 2007, p.23). Aquilar (2009) stated in his opening speech to First International Conference for Investment Advisors, "*As regulators of investment advisers, we have a critical role to play. Investors place their trust in us to work diligently to protect their interests."*

Regulation alone cannot protect investors from dishonesty or misconduct by financial institutions. Effective corporate governance that focuses on both prevention and deterrence of fraud is necessary to combat fraud (Coburn 2006, p.349).

Onsite visits to investment managers are one of the supervisory tools that are used by financial services regulators. These visits are regarded as a minimum requirement placed on regulators by organisations such as the International Monetary Fund ("IMF") to ensure effective regulation (Tieman & Cihák 2008, p.43).

International regulatory bodies such as the International Organisation of Securities Commissions ("IOSCO") do not directly require regulators to implement a risk-based approach to supervision. It merely mentions that regulators should be risk adverse (Stewart 2005, p.44). Stewart (2005, p.43) remarks that the Financial Services Authority in the United Kingdom ("FSA") and other regulators have started to focus more on risk-based approaches in the regulation of financial institutions. The FSA have specific regulatory objectives that include reducing financial crime and protecting the consumer. By following a risk-based approach to regulation, they strive to ensure that through applying risk management techniques in their regulation they meet these objectives (Stewart 2005, p.46). In terms of the risk-based approach that the FSA follows, they perform onsite visits to the firms that pose the highest risk to their objectives (Capps & Linsley 2001, p.250).

The FSB follows a risk-based approach similar to the FSA in supervising investment managers. In the approach the risk that individual financial institutions posses on the FSB's regulatory objectives is measured and mitigated on continuously (FSB 2010, p.2).

The FSB is in terms of its risk-based approach to supervision expected to proactively identify risk inherent to entities it regulate which include the identification of any issues that will influence the integrity of the investment manager such as possible fraudulent investment schemes (FSB 2008, p.27).

The onsite visits to investment managers entails scrutiny of investment manager's businesses. The onsite visit team review all aspects of the investment managers business and then rate the risk of the specific areas that impacts on their regulatory objectives. During the process, the onsite visit team perform a series of interviews, scrutinise documentation and do sample testing to ensure safekeeping of investor's funds (Millard & Hattingh 2010, p.128). The focus of onsite visits is to identify conduct that may lead to non-compliance of legislation proactively and might therefore detect possible investment fraud schemes (FSB 2007b, p.11).

An onsite visit is in some ways similar to proactive fraud auditing. The fraud auditor searches for fraud even where there are no allegations that fraud exist (Vona 2008, p.19). When regulators perform onsite visits on regulated entities they must always consider the

possibility that fraud may exist and if undetected can lead to failure of achieving one of their main objectives namely investors protection (Bales & Fox 2009, p.5).

To achieve this objective the regulator might have to adopt alternative techniques in its onsite visit of investment managers. In this regard this study will evaluate whether the fraud auditing approach to identify management fraud as described by authors such as Vona (2008) and Singleton *et al* (2006) can be adapted by the regulator of investment managers to improve the possibility to detect investment fraud schemes.

1.1.4 A fraud auditing approach

Fraud auditing can be defined as an approach where the goal is to offer an opinion on the existence of fraud (Vona 2008, p.70). Financial auditing provides reasonable assurance relating to the reliability of financial statements (Rezaee 2002, p.218) and "*rely on the adequacy and effectiveness of internal controls to detect fraud*" (Rezaee 2002, p.1).

Singleton *et al* (2006, p.43) draw the distinction between financial auditing and fraud auditing. Financial auditing is more procedural and looks at overt aspects (structural considerations) such as: hierarchy, financial resources, goals of the organization, skills and abilities of personnel, technology utilised, performance standards and efficiency measurement. Fraud auditors in addition to overt aspects look at covert aspects (behavioural considerations), such as the mindset of the person, which is displayed in his attitudes, feelings, values, norms, interaction, supportiveness and satisfaction (Singleton *et al.* 2006, p.43). The structural considerations are visible and can be identified easily while behavioural considerations are hidden and are not easily detected. Therefore the professional scepticism tends to play a more important role in fraud auditing where substance over matter is questioned (Singleton *et al*. 2006, p.43).

Fraud auditing is different from fraud investigations. The purpose of fraud audit is to proactively look for weaknesses in an organization's internal control structures and determine whether there is opportunity to exploit these weaknesses. Fraud investigations on the other hand examine the fraudulent activity after it occurred (Cendrowski et al. 2007, p.52).

1.1.5 Fraud auditing techniques that can be used in regulatory supervision

Regulatory onsite visits are proactive and as such cannot be regarded as investor fraud investigations. The regulator however wants to ensure that they identify indicators if investor fraud exists (Millard & Hattingh 2010, p.152).

When considering the impact of increased regulation or supervision one needs to take into consideration that not all investments are fraudulent. It is therefore important that the regulatory personnel that perform onsite visits are trained and able to apply fraud auditing techniques that will assist in identifying possible red flags (Tieman & Cihák 2008, p.43). An effective fraud auditor must be able to consider human and individual, organizational, cultural, motivational, economic and competitive, social, regulatory as well as accounting, audit and internal control perspectives (Singleton *et al*. 2006, p.50).

Pressman (1998, p.414) argues that *"empirical psychology, which emphasizes how people make choices in a world characterized by uncertainty, provides a more plausible explanation for why financial fraud is so prevalent"*. This is an interesting theory that Pressman (1998, p.414) combines with the behaviour of persons committing the fraud. Cases of financial fraud involve individuals with charming and convincing personalities. As such it changes the dimension of how investment fraud schemes can be detected. It requires the fraud auditor searching for signs of fraud to not only follow the money but also looking into the behavioural indicators (Singleton *et al*. 2006, p.107).

It is therefore important that the regulator can identify common signs (red flags) that indicate the existence of investment fraud.

1.2 THE RESEARCH PROBLEM

Although there are various academic books [(Albrecht 2003), (Cendrowski *et al*. 2007), (Golden, Salak & Clayton 2006), (Rezaee 2002), , (Vona 2008) and (Wells 2008)] relating to the use of a fraud auditing approach (techniques and red flags) by external, internal and forensic auditors, limited research is available that specifically focus on regulators using

the approach when supervising financial institutions. The available academic resources mainly focus on the detection (using fraud auditing techniques and red flags) of management fraud and not on the detection of investment fraud.

In this study, the fraud auditing approach applicable to management (financial statement) fraud will be evaluated and applied to investment fraud to determine if it can be used by the regulator as part of its risk-based onsite visits methodology to improve the likelihood of detecting investment fraud proactively.

1.3 PURPOSE STATEMENT

The main purpose of this study is to evaluate whether the regulator (as part of the risk-based supervision methodology they apply in the supervision of investment managers) can use a fraud auditing approach (similar to those used in the identification of management fraud) to identify the existence of investment fraud schemes devised by investment managers. In addition, determine whether the regulator in terms of its mandate have the authority to do so, need to change its methodologies and might have to consider improving the skill set of its employees.

1.4 RESEARCH OBJECTIVES AND QUESTIONS

1.4.1 Primary objective

The primary objective of this study is to evaluate the applicability of a fraud auditing approach used in the detection of management fraud to the regulatory environment and in particular investment fraud schemes.

1.4.2 Secondary objectives

The secondary objectives of this study are: to describe investment fraud schemes that can be devised by investment managers; evaluate the similarities between investment fraud schemes and management fraud; describe the business of investment managers and the regulatory environment it operates in; evaluate the best practise relating to risk-based supervision and onsite visits of investment managers issued by the IOSCO and

international financial services regulators in particular the FSA and SEC; review the literature relating to fraud auditing approaches that can be used to detect management fraud; consider the applicability of a fraud auditing approach to the supervision of investment managers and detection of possible investment fraud; review the literature relating to red flags and fraud auditing techniques indicating management fraud; and to identify the red flags and auditing procedures and techniques that can be used by the regulator to detect investment fraud schemes.

1.5 IMPORTANCE AND BENEFIT OF THE PROPOSED STUDY

The recent increase of investment fraud schemes internationally and in South Africa has left regulators open for criticism of not detecting these fraud schemes timeously. Questions are asked why regulators fail to identify fraud proactively and why investment managers get away with fraudulent activities without being detected (Aquilar 2009).

This study will evaluate whether the fraud auditing approach applicable to the detection of management fraud can be applied to investment fraud. The study will also consider whether the approach can be used in the regulatory environment in particular, the detection of investment fraud schemes by the regulator during its risk-based supervision onsite visits.

1.6 RESEARCH METHODOLOGY

The study will be done through an extended research literature review. A literature review can be described as an effective evaluation and synthesis of academic literature and research. Baumeister and Leary (1997) view literature reviews as vital for "*bridging the gap of interpretation*".

Hofstee (2006, p.121) indicates that extended literature reviews "*cannot produce anything substantially new*" as they can only "*produce a new perspective on what has gone before*". Mouton (2001, p.190) holds the view that a literature review can only summarise and organise existing scholarship. Baumeister and Leary (1997) hold a different view from Hofstee (2006, p.121) and Mouton (2001, p.190) as they describe an extended literature

review as a "*valuable theory building technique*" and classify these types of studies in several categories of which they view the "*most ambitious goal*" of such a review studies that involve "*theory development*". Mouton (2001, p.190) is in agreement with Baumeister and Leary (1997) that these insights or theory development need to be supported by empirical studies to test the theory that was reached in the literature review.

This study indicates that there is limited research done on fraud auditing relating to investment fraud. There is however substantial research and academic publications on fraud auditing relating to management fraud.

Hofstee (2006, p.121) indicates that an integral part of an extended literature review is to review the various specialities, a field or sub field fragmented into and then to link it together. This study will focus on the field of fraud auditing and will identify the fraud auditing techniques used in this field. It will identify the fraud auditing techniques that are used in the sub field of management fraud and will relate this information to sub field of investment fraud.

The study will focus on investment fraud schemes devised by investment managers. *Firstly*, investment fraud schemes will be defined by referring to academic research on the topic. *Secondly*, the scope and process that the FSB follows to perform risk-based onsite visits to investment managers will be described. It will be evaluated against best international practises prescribed by IOSCO to obtain an understanding of how onsite visits relate to fraud auditing.

Thirdly, research relating to fraud auditing techniques and the identification of red flags that indicate the existence of management fraud will be considered. *Lastly*, the techniques identified in the literature will then be critically analysed to evaluate and identify the red flags and fraud auditing techniques that can be used when the FSB evaluate the business of investment managers to identify investment fraud schemes. As suggested by Baumeister and Leary (1997) this will be a "*theory building exercise*".

The research literature consists of academic literature and research that specifically focus on fraud auditing techniques and its importance. The study will focus on resources that are not older than ten years except where the secondary resources refer to primary

resources or resource relates to a specific field of financial statement analysis and regulation. *Firstly*, several academic books of the following authors: Albrecht (2003), Cendrowski *et al*. (2007), Coenen (2008), Iyer and Samociuk (2006), Singleton *et al*. (2006), Vona (2008) and Wells (2008), relating to the topic of fraud auditing was identified as the starting point for preliminary literature review. These books offer a wide variety of examples regarding the use of fraud auditing to identify management fraud. As the study will evaluate these techniques in relation to investment fraud there is ample resources available relating to fraud auditing techniques and red flagging as it related to management fraud schemes that can be compared.

Secondly, the book of Sander (2009) on the Madoff Ponzi scheme was considered to get an understanding of the different red flags that existed in one of the world's largest investment fraud schemes.

Thirdly, academic search engines and databases were mined for articles, including both South African and international journals and databases were used to search for academic literature containing the term "***fraud***". The search was then narrowed to the following key words: "***fraud auditing***", "***fraud examinations***", "***forensic accounting***", "***forensic investigations***", "***investor fraud***", "***embezzlement***", "***securities fraud***", "***investment manager/investment advisor***" in conjunction with "***fraud***", "***investment fraud schemes***" as well as "***fraud auditing***", "***fraud deterrence***", "***investigative accounting***", "***red flags/flagging***". From these searches several academic journal articles were identified that relate to fraud auditing, red flags relating to management fraud as well as articles that deal with securities fraud that is related to investment fraud schemes.

As stated above there is limited academic literature relating to the use of fraud auditing and red flags that regulators use to identify investment fraud schemes proactively. Gadinis (2008) provide some information on supervision techniques such as onsite visits that regulators perform. Evola and O'Grady (2009) and van de Bunt (2010) provide some insight on investment fraud schemes and red flags for investors that can be adapted and used by regulators.

Fourthly, best practise relating to the regulation of investment managers issued by the IOSCO was obtained from its website. The guideline in these papers is broad and does

not give specific detail relating to techniques used to supervise investment managers. Further information relating to regulation of investment managers with specific reference to risk-based supervision was obtained from search engines mentioned above as well as the websites of the FSA and SEC. *Lastly*, papers provided by the SEC during the First Annual Conference for Investment Advisors (managers) that took place from 23 to 26 June 2009 in Washington DC were considered.

There exists enough research literature to evaluate the problem statement of the study that fraud auditing and red flags can be used during regulatory onsite visits to detect investment fraud schemes devised by investment managers.

1.7 DELIMITATIONS AND ASSUMPTIONS

The study will be done with the following delimitations and assumptions. The relevance of a fraud auditing approach in relation to only regulated investment managers will be considered. The study will be limited to a fraud auditing approach including the audit procedures, techniques and red flags used to detect management fraud and a comparison of how these can be used to detect investment fraud schemes devised by investment managers.

The international best practise will be limited to research of the principles of IOSCO as this is the only international financial services regulatory body applicable to the legislation that regulate investment managers in South Africa. The comparison of risk-based supervision methodology followed by the FSB with other regulators' methodology will be limited to the FSA and SEC as these regulators' are regarded as the leaders in relation to the regulation of investment managers. The study will not include investment fraud schemes relating to market manipulation or insider trading. These abuses are investigated in terms of the Securities Services Act (36/2004) by the Directorate of Market Abuse of the FSB and do not fall within the ambit of the supervision of investment managers in terms of the FAIS Act (37/2002).

1.8 CHAPTER OUTLINE

1.8.1 Chapter 2: Defining investment fraud schemes

The study will focus on investment fraud, and as such a definition for "investment fraud" will be formulated by evaluating different definitions in the academic literature, as well as regulatory international best practice. **Chapter 2** will aim to arrive at an acceptable academic definition for investment fraud. Baumeister and Leary (1997) suggested that in a literature review the researcher must "*present a full and vigorously integrative theoretical framework early*" in the work. The chapter will therefore set the theoretical framework for evaluating investment fraud schemes. Specific examples of investment fraud that have occurred internationally, as well as in South Africa, will be described to set the background for the rest of the study.

The similarities between investment fraud schemes and management fraud will also be discussed, as this will form the basis for the comparative work that will be done in **Chapter 5** in relation to the fraud auditing procedures, techniques and red flags.

1.8.2 Chapter 3: The supervision of investment managers and risk-based onsite visits

Investment fraud schemes are a broad concept, and this study will concentrate on the investment management industry specifically. **Chapter 3** will review the concept of the supervision and regulation of investment managers – to provide the reader with a context on the regulation, the mandate and role of the regulator to protect investors against fraudulent financial institutions.

The concept of risk-based supervision will be explained and the processes followed by different regulators – when conducting onsite visits – will be compared. The methodologies will be evaluated in relation to international best practices: the best practices followed by financial regulators, such as the FSA in the UK and SEC in the USA, and how these apply to the regulation of investment managers in South Africa.

1.8.3 Chapter 4: The use of a fraud auditing approach

Chapter 4 will critically evaluate the academic literature available relating to fraud auditing and how this differs from fraud investigations. An approach to fraud auditing and its relevance to the supervision of investment managers will be considered – with specific reference to the process that regulators follow, as discussed in **Chapter 3**.

1.8.4 Chapter 5: The applicability of a fraud auditing approach in detecting investment fraud schemes

In **Chapter 5**, the fraud auditing approach, as discussed in **Chapter 4** will be applied to the detection of investment fraud schemes. Concealment strategies, red flags and audit techniques that can be used for the detection of management fraud will be considered, and then their applicability to investment fraud schemes will be discussed.

1.8.5 Chapter 6: Conclusion: on the use of a fraud auditing approach in detecting investment fraud

In **Chapter 6**, the findings will be summarised and a conclusion will be drawn on whether a fraud auditing approach can be used by the regulator to detect investment fraud. Recommendations are made on the possible improvement of the risk-based supervision onsite-visits process. Lastly, a summary of the contributions of the study, and further possible research avenues in the field will be suggested.

CHAPTER 2:
DEFINING INVESTMENT FRAUD SCHEMES

2.1 INTRODUCTION

A definition for the specific type of fraud that involves investor funds will be explored in this chapter. According to the Oxford Dictionary, the term "define" is to state precisely the meaning of a word or term (Pearsall 1999, p.376) . Therefore, a definition is a statement of meaning. Seeing that different authors have different explanations for the meaning of the term "investment fraud", it becomes necessary to define it in the context relating to the corporate environment.

To give background to the definition of investment fraud in this chapter, the general concept of white-collar crime and fraud as they relate to the corporate environment will be explored – *firstly*, from a legal and auditing perspective. *Secondly*, types of fraud will be explained. *Thirdly*, examples of international and South African investment fraud will be given. *Lastly*, investment fraud for the purposes of this study will be defined.

2.2 DEFINING FRAUD

2.2.1 White-collar crime

The term fraud has been "*traditionally referred to as white-collar crime*" (Singleton *et al*. 2006, p.8). White-collar crime is the general term used for crimes committed by or against businesses by people in positions of trust (Singleton *et al*. 2006, p.7). Ivancevich *et al.* (2003, p.114) mention that Edwin H. Sutherland was the first to introduced the term "white-collar crime" in the 1940s, when he defined this as "*crime in the upper or white-collar class, composed of respectable, or at least respected businesses, and professional men… It consists of violations of delegated or implied trust…*"

The Oxford dictionary defines white-collar activities as "…*of or relating to the work done or people who work in an office or other professional environment*" (Pearsall 1999, p.1632). Singleton *et al*. (2006, p.7) describe white-collar crime as fraud, which they define as "*lying and cheating"*, as well as "*theft and embezzlement*". These activities comprise fraudulent

acts where deception is common. White-collar crime is generally referred to as corporate fraud (Coenen 2008, p.144).

For the purpose of this study, "White-collar crime" will be defined as fraudulent (deceitful or dishonest) acts, perpetrated by people in positions of trust, who work in an office or other professional environment. Such acts are intended to result in a financial or personal gain and are synonymous with fraud.

The Oxford Dictionary defines fraud as, "…*wrongful or criminal deception intended to result in a financial or personal gain";* and fraudulent as, *"deceitful or dishonest*" (Pearsall 1999, p.562). To prove that fraud exists – and in order to prosecute the person committing a fraud, it is important to consider the legal definition and the individual elements of fraud.

In this study, fraud will, firstly, be defined from a legal point of view – followed by an auditing and professional point of view – to give clarity on the approach to investment fraud.

2.2.2 Definitions and elements of fraud

Snyman (2007, p.520) defines fraud from a **legal point of view,** as "…*the unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another*". Snyman (2007, p.520) indicates that to prove that a fraud has been committed, the elements of misrepresentation, prejudice or potential prejudice, unlawfulness and intention must be present.

The core element in the definition above is "misrepresentation". Misrepresentation is a wide concept and can include acts such as concealment, non-disclosure, false representations, deceit, "*perversion or distortion of the truth"* or trickery (Wells 2008, p.9). For instance, fraud in relation to business transactions would be the intentional and deliberate concealment of the true nature of the transaction (Vona 2008, p.6). Snyman (2007, p.521) states that the misrepresentation can be expressed or implied, through a positive act or an omission, and can be about past or present events, or even false promises about the future.

For fraud to be committed, prejudice or potential prejudice must always exist (Snyman 2007, p.524). Coenen (2008, p.7) defines fraud from a legal perspective as "…*an intentionally false misrepresentation about a material point*", which causes the victim of the fraud to suffer harm. To prove that fraud has been committed, the harm suffered by the victim does not need to be actually prejudiced, as long as there is a reasonable possibility that the victim could be prejudiced then fraud can be proven (Snyman 2007, p.525).

It is important to note that the person to whom the misrepresentation was made does not necessarily have to be prejudiced. If a third party relies on the misrepresentation and is prejudiced, then it would be sufficient to prove this element of the crime (Snyman 2007, p.525).

The act of misrepresentation must be unlawful; if a person merely obeys an order, there could be possible grounds for justification (Snyman 2007, p.527). Lastly, there needs to be the intention to defraud. This means that the person making the representation must know that it is false or holds "…*no honest belief in its truth*". If he/she then acts recklessly, and is careless as to whether it is true or false – or if he/she doubts the facts, but does not check their correctness, then such an individual must be held responsible for his/her actions (Snyman 2007, pp.527-528).

If a person makes an unintentional error by, for instance, entering an incorrect number in financial statements, this would not be fraud (Albrecht 2003, p.6).

As this study will consider fraud auditing techniques, it is necessary to understand fraud from an **auditing perspective**.

In statement 240, of the International Standard on Auditing ("ISA 240"), fraud is defined as "*an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage*" (IFAC 2010, p.159).

ISA 240 indicates that auditors are involved in identifying fraud that causes a material misstatement in financial statements, especially if they "*do not make legal determinations*

on whether fraud has occurred." The statement further identifies **two** types of fraud that can be committed, namely: management and employee fraud (IFAC 2010, p.157).

2.2.3 Classifying the different types of fraud

Albrecht (2003, p.7) divides fraud into "*those committed against an organisation*", such as occupational fraud, and *"those committed on behalf of an organisation"* as management fraud.

Albrecht (2003, p.7) further classifies fraud into the following **six** types: *Firstly*, there is occupational fraud, where employees of the organisation are involved. *Secondly*, management fraud; and *thirdly,* investment scams which are closely related to management fraud, and where individuals trick investors into investing in fraudulent investments. Albrecht classifies a variety of fraud schemes, such as telemarketing fraud, Ponzi schemes, prizes/sweepstakes, credit-card offers, work-at-home schemes, advance-free loans, telephone slamming, telephone cramming and investments under investment scams. *Fourthly*, there is vendor fraud - where organisations that sell goods or services overcharge, or fail to ship the goods. *Fifthly*, there is customer fraud, where the customers deceive organisations into giving them something that they should not have or persuade them into charging them less. *Lastly*, there is miscellaneous fraud, where fraud other than financial gain, does not fall into any of the other categories.

Comer (2003, p.5) defines fraud as, "…*any dishonesty through which one person intends to gain an advantage over another*", and people exploit processes with the intention of getting their greedy hands on assets, both tangible and intangible. Comer (2003, p.5) classifies corporate fraud as being of the following **five** types: *Firstly*, corruption that can be described as the payment of unauthorised benefits for performing or not performing a specific task. *Secondly*, there are those conflicts of interest, where employees have "*private, undisclosed interests that could interfere with their work and fiduciary obligations*" to their employer. The *third* type is the "*theft of assets*". This includes theft, embezzlement, and the misuse of assets, false accounting and deception.

Fourthly, false reporting that includes creating false records and the suppression of material information. *Lastly*, there is technology abuse. This includes unauthorised access to computer systems by employees and other computer-related fraudulent activities.

From the above classification, it becomes evident that there are many types of corporate fraud. This study will only focus on what Albrecht (2003, p.9) describes as investment fraud scams – together with elements of other fraud, such as conflicts of interest and false reporting. It will further examine whether fraud auditing techniques used to detect management fraud can identify investment fraud. It is, therefore, necessary to consider management fraud.

Crendrowski *et al.* (2007, p.33) describe management fraud as fraudulent financial reporting through the manipulation, falsification or alteration of documents of record, misrepresentations, omissions and the misapplication of generally accepted accounting principles. Management fraud is also referred to as financial statement fraud (Singleton *et al*. 2006, p.28). Singleton *et al.* (2006, p.2) define management fraud as the intentional misrepresentation of an entity's performance done by persons in management roles for their own benefit – to obtain status or economic incentives, such as promotions or bonuses.

2.3 FRAUD COMMITTED BY PERSONS IN POSITIONS OF TRUST

As management fraud is normally committed by persons in positions of trust, they have the authority to override controls (Singleton *et al*. 2006, p.2). The Oxford Dictionary defines "trust" when used as a noun, as the "*firm belief in someone or something*", or the "*acceptance of the truth of a statement without evidence or investigation*" (Pearsall 1999, p.1540). When trust is used as a verb, it is defined as a "*belief in the reliability, truth, ability or strength of*" something – or when trusting someone with something, so as to "*have the confidence to allow someone to have, use or look after it*" (Pearsall 1999, p.1540).

Singleton *et al.* (2006, pp.17-19) state that in the corporate environment any "*person in a position of trust has authority over people or the property of the organisation*". This gives

them "*certain duties, obligations and responsibilities, such as the honest, diligent, and prudent care, protection and preservation of the property by the person to whose custody it has been entrusted*." Persons in a position of trust normally have control over decision-making, and it is easy to commit management fraud, such as falsifying the financial records of a company (Cendrowski *et al.* 2007, p.263).

As with management fraud, investment fraud is normally devised by persons in positions of trust (Ivancevich *et al.* 2003, p.119). Albrecht (2003, pp.9-10) describes investment fraud as schemes where fraudulent and usually worthless investments are sold to unsuspecting investors. When investors purchase financial products, such as shares, they place trust and confidence in the directors, managers, securities markets, regulatory bodies, laws and politicians (Ivancevich *et al.* 2003, p.119). Investment managers are entrusted with the funds and/or management of their client's assets, and as such, must ensure that this does not breach their fiduciary duties (Financial Institutions (Protection of Funds) Act 28/2001, sec.2).

The Oxford Dictionary defines 'con' as "*deceiving (someone) into doing or believing something by lying to them*" (Pearsall 1999, p.294). To be 'conned' you have to "*trust the person that is trying to deceive"* you (Albrecht 2003, p.6). According to Albrecht (2003, p.6), investment fraud schemes are also referred to as Ponzi schemes (see **paragraph 2.4.2** below). These schemes have certain fundamental concepts that can be used to describe any type of fraud. The concepts are deception, greed by the perpetrator, as well as by the investors, together with an element of confidence, all of which may be observed in typical Ponzi schemes (Albrecht 2003, p.7).

Økokrim (in Gottschalk 2010, p.449) describes fraud relating to investors, as financial fraud. In this type of fraud, investors are deceived into investing in financial instruments that are portrayed as yielding high profits, but since the money is never invested, and the instrument does not exist, the investment cannot produce the promised profit, and usually the money is stolen by the person devising the scheme.

To better understand the concept of investment fraud and the typical characteristics of these schemes, specific examples of international and South African schemes will now be

discussed. These were chosen to illustrate the history of investment fraud and how it has developed over time.

2.4 SPECIFIC EXAMPLES OF INTERNATIONAL INVESTMENT FRAUD SCHEMES

The following are brief summaries of examples of some of the most publicised international fraud schemes in history – where investors were deceived in some way or another.

2.4.1 The South Sea Bubble

Singleton *et al*. (2006, p.36) indicates that the scheme devised by the South Sea Company was the first corporate fraud in history where investors were mislead. In 1710, the British Government granted the South Sea Company the rights to trade (conduct business). In return, the company had to exchange shares in the company for government paper that was trading at a discount, and not even guaranteed by the parliament. The government undertook to pay the company interest at a low rate. The South Sea company did not do any real business, apart from a few unsuccessful ventures in the slave trade.

The investors were probably attracted by the trading prospects, the company's financial operations on behalf of the government, or the fact that the company generated substantial amounts of cash. This was believed to be an indication that it could make profits in the trading environment (Jarvis 2000, p.14).

The company, however, traded in its own shares – by lending the shareholders money, with their shares in the company as security. This enabled them to purchase more shares in the company. The money was borrowed from a client's bank and from the government. The investors of the South Sea Company were the English aristocrats, and even the king himself invested some money (Jarvis 2000, p.14).

The price of the shares initially rose, due to speculative buying, but when the people started selling, the company was unable to pay dividends and was subsequently declared bankrupt. The politicians that were involved were out of office, and the parliament voted to

seize the assets, including those of the corrupt politicians. The unwinding process took the appointed trustees seven full years, and they realised two million pounds. The government did take back the debt and paid out the shareholders, but this did not apply to those who had speculated and lost their investments (Jarvis 2000, p.14).

Jarvis (2000, p.15) states that the South Sea Company was not strictly a pyramid scheme due to the fact that the government was involved and no actual returns were paid when the speculation took place. Certain features of the scheme resemble a pyramid scheme, such as the fact that a return to the investors was generated from the rising share price that was generated by money from new investors. Secondly, the increase in the price was done through the misrepresentations of the operators.

For the first time in history, an outside auditor, Charles Snell, was brought in to examine the books of the South Sea Company. This marked the start of Chartered Accountants in England (Singleton *et al*. 2006, p.36).

2.4.2 Charles Ponzi

Ponzi schemes are named after Charles Ponzi who is regarded as the father of investment fraud schemes (Albrecht 2003, p.6). Charles Ponzi devised a scheme in 1919, when he claimed to invest in international postal-reply coupons. Immigrants to the USA used these coupons to pay postage on international mail. These coupons were traded at widely varying values in different countries, due to the currency fluctuations during World War I (Jarvis 2000, p.15).

Ponzi claimed that he could make 40% return on investments in 90 days. He had approximately 17 000 investors. The investigations found that although he did pay a few of the investors out, he had only purchased $30 worth of coupons (Sander 2009, p.13).

Ponzi schemes are defined as, "…*any investment swindle in which early investors are paid with funds received from later investors*" (Ivancevich *et al*. 2003, p.115), and where "*artificially high returns are paid to earlier investors*" (Jarvis 2000, p.15). The Oxford Dictionary definition of Ponzi schemes is as follows: "…*a form of fraud in which belief in*

the success of a non-existent enterprise is fostered by the payment of quick returns to the first investors from money invested by later investors" (Pearsall 1999, p.1112).

Sander (2009, p.1) points out that the term "Ponzi scheme" is an American colloquialism for pyramid schemes. Jarvis (2000, p.15) recognises deception, greed and confidence, which con people into investing (Albrecht 2003, p.6) in his description of pyramid schemes. Here, he identifies the following **four** typical stages of a pyramid scheme:

Firstly, investors are canvassed by advertising "*high interest rates or huge capital gains after a short period*". Most pyramid schemes have a gimmick that is usually "*based on some real or imagined market inefficiency or loophole in the law*."

Secondly, the investors tell others of the high returns and more people invest. The new investors initial capital is then used to pay interest; and, if necessary, capital to the early investors. In many cases, the early investors then reinvest their capital, and sometimes their interest, as they want to make even more money. In this stage, most people are still sceptical about the scheme that might appear too good to be true.

Thirdly, the scheme builds up a good reputation by paying interest, and when requested the capital as well. This removes the doubts of even the sceptics of the scheme, and as such, even more people invest in the scheme. Even some of the sceptics that still think it is a fraud scheme invest – in the hope of making some money themselves. The scheme therefore appears to be successful for a period of time.

Lastly, the interest and capital due to the initial investors starts exceeding the money that the scheme generates from new investors – and then the scheme collapses. When payment is interrupted, investors try and get out their money but without any success – as this money has been paid to the initial investors in interest. The scheme normally has some assets or investments that are used to make the scheme appear creditable, but this is usually not enough to cover the capital invested. In some instances, the cash invested has been stolen outright by the operators, or used to pay exorbitant commissions or salaries to the operators and the staff.

2.4.3 Investors Overseas Services ("IOS")

In the 1960s, Bernie Cornfield and Edward M. Cowett, through their company IOS that was founded in Panama and based in Switzerland, created an offshore "fund of funds" (Ivancevich *et al.* 2003, p.116) that would collect more than one billion dollars in investors' funds (Raw C., Page B. & Hodgson G. 2005, p.4). The fund was sold initially to US expatriates who wanted to avoid US income tax, but later sold by approximately 25 000 salespersons, calling themselves "financial counsellors" (Raw *et al.* 2005, p.98). They sold the funds on a door-to-door basis all over Europe. The offering was very popular and the Cornfield sales pitch was: *"Do you sincerely want to be rich?*" They did this primarily by creating a vehicle for investors in the USA to avoid income tax. Investors bought shares in IOS, while the money was then invested in other IOS funds (Ivancevich *et al.* 2003, p.116).

The fund came to a downfall in 1969, when it made a public offering due to the investors who wanted to cash in their "paper fortunes". IOS then reallocated to Canada. The public offering did not help, as the money raised by the company was used by Cornfield to diversify; and it created a cash shortage. At this stage, Robert Vesco offered his help to Cornfield – but he then went on to take over IOS, and got rid of Cornfield. Vesco then transferred more than $200 million of cash belonging to IOS funds to his own ventures in South America. Following complaints from the SEC, the Canadian authorities liquidated IOS and all the entities (Raw *et al.* 2005, p.205).

Raw *et al.* (2005, p.5) indicated that the scheme, through its offshore presence in various jurisdictions, managed to conduct business that would be regarded as illegal if the entities had been based in one jurisdiction only. Raw *et al.* (2005, pp.5-6) listed the following fraudulent activities that IOS committed when Cornfield and Cowett were in control:

Firstly, client's money that was supposed to be held in trust was utilised to fund "*financial manoeuvres for the benefit of the IOS itself, its directors and employees and their friends*." *Secondly*, the IOS sales force was involved in illegal currency transactions. *Thirdly*, the IOS misrepresented its largest fund investment performance. This was then used to attract millions of investors. *Fourthly*, the IOS Fund of Fund's basic nature was disguised, in that although, it was supposed to provide the investor with investment diversification, it merely charged the investors double fees for doing nothing of the sort.

Fifthly, the funds invested clients' money in unmarketable shares. These shares were often those used by the IOS to make profits for its own benefit. *Sixthly*, IOS invested in oil and gas rights in the Canadian Arctic, and then paid itself almost $10 million to "*revalue*" the rights. *Lastly*, the IOS sold shares to its own funds, in addition to $100 million shares to the public on the basis of fraudulent prospectuses that contained omissions and misrepresentations. The cash raised in the share transactions was used for the "*personal benefit of the directors of IOS*".

From the above discussion, it may be seen that the "*IOS presented to be creating wealth for the many, when it was really making money for the few*" (Raw *et al.* 2005, p.6).

2.4.4 Hedge fund investment fraud

Hedge funds are described as risky investments. The worst fear of investors in hedge funds is fraud (Shain 2008, p.284). McCrary (2002, p.7) uses the President's Working Group on Financial Markets definition of hedge funds. This that states a hedge fund is "*a pooled investment vehicle that is privately organized, administered by a professional management firm …. and not widely available to the public.*" Gottshcalk (2010, p.449) notes that a common feature of hedge funds is that the *"fund managers often invest a considerable amount of their own wealth in the funds they manage and generally lock up clients' capital for a few weeks or months and in some cases even years.*"

The performance-based compensation structures with which hedge funds remunerate their managers – in the correct circumstances, especially where managers have control over the funds – actually encourages fraud (Longo 2009, p.317). In the USA alone, the SEC brought to book more than 51 cases of hedge fund fraud, from 2000 to 2005, involving approximately $1.5 billion (Stulz 2007, p.188).

Muhtaseb and Yang (2008, pp.182-201) describe five cases of fraud committed by hedge fund managers and identifies the variations of such fraud in hedge funds. Utilizing clients' funds invested for the hedge fund, the manager's business enterprises (Bayou Funds and Maricopa Investments), value the hedge funds in such a way that they show positive

returns to disguise any losses (Beacon Hill Asset Management), any misrepresentation of performance (Lancer Group), or false client statements (Maricopa Investments).

Reuters published an article on 29 June 2009: "*Madoff gets 150 years for massive investment fraud."* Here, they described Madoff as committing "*extraordinarily evil*' *crimes in Wall Street's biggest and most brazen investment fraud.*" (McCool & Graybow 2009, p.1). Bernie Madoff was arrested on 11 December 2008, when he admitted to the FBI that *"he personally traded and lost money … clients…he 'paid investors with money that wasn't there'…he was 'broke' and 'insolvent' and that he had decided that 'it could not go on'"* (Sander 2009, p.123).

Bernie Madoff, a former chairman of the NASDAQ, was a reputable investment manager that ran a hedge fund (Sander 2009, p.37). He managed to defraud hundreds of wealthy individuals and charitable organizations of more than $65 billion dollars. Sanders (2009, pp.111-112) quotes the complaint filed by FBI Special Agent, Theodore Cacioppi, as follows:

> *"BERNARD L. MADOFF, the defendant, unlawfully, willfully, and knowingly… did use and employ manipulative and deceptive devices in violation of [the act listed above] by (a) employing devices, schemes, and artifices to defraud; (b) making untrue statements of material facts and omitting to state material facts necessary, in order to make the statements made …and (c) engaging in acts, practices, and courses of business which operated and would operate as a fraud and deceit upon persons, to wit, MADOFF deceived investors by operation securities business in which he traded and lost investors' money, and then paid investors purported returns on investments with the principal received from others, different investors, which resulted in losses of approximately billions of dollars."*

The types of fraud described above are not exclusive to hedge funds, and are a good indication of the type of fraud investment managers might commit (Muhtaseb & Yang 2008, p.180).

2.5 INVESTMENT FRAUD SCHEMES IN THE SOUTH AFRICAN FINANCIAL SERVICES INDUSTRY

The South African financial services industry, as mentioned in **Chapter 1**, has not been without its own scandals. Several alleged investment fraud schemes construed by regulated investment managers will now be discussed.

2.5.1 Common Cents Investment Portfolio Strategists and Ovation Global Investment Services

Ovation was an investment manager and linked-investment services provider. They offered the general public easy access to mainly collective investment schemes. Clients would give Ovation instructions to buy or sell collective investment schemes on their behalf. The collective investment schemes were then registered in the name of Ovation Nominee (Pty) Ltd ("Ovation Nominee") and held on behalf of the client. The benefit for the client to utilise their platform was to have a single entry point to switch between different collective investment scheme management companies (Peterson & Levin 2007, pp.4-5).

Cornerstone Transaction Financing (Pty) Ltd was the shareholder of Ovation, a company owned by Mr Cruickshank. Mr Cruikshank was also the shareholder of Common Cents, an investment manager who ran an unapproved collective investment scheme commonly referred to as the Common Cents "cash pools" (Peterson & Levin 2007, pp.5-6).

Mr Cruickshank managed to convince investment advisors to invest their clients' cash in the Common Cents' cash pools offered on the Ovation platform. This appeared to be a legitimate money market investment managed by an approved investment manager on a regulated platform. Clients received investment statements in which Ovation reported that the investments were held by its nominee. The information reported to clients was not correct, as Mr Cruickshank provided false information relating to the returns on the "cash pools" to Ovation's staff to include in the statements (Peterson & Levin 2007, p.14).

In actual fact, the money was allegedly channelled from the Common Cents' bank account to Mr Cruickshank's private bank account, and to bank accounts of other businesses with

which he was involved, in addition to some of his associates' bank accounts. When the bank account of Common Cents was closed by its bankers, Ovation continued to make redemptions with funds from new investors, or from the funds of other clients, and as such, a "hole" of R42 million was created in Ovation Nominee.

Common Cents misappropriated approximately R190 million from the middle of 2005 until the end of August 2006, when Ovation's auditors KPMG reported to the FSB that they had reason to believe that certain irregularities were taking place in the conduct of Ovation relating to the Common Cents "cash pools" (Peterson & Levin 2007, p.14). The FSB reacted, and based on the information of the auditors together with an investigation, applied to the High Court to place Common Cents under curatorship (FSB 2006).

The curatorship was superseded by the ostensible suicide of Mr Cruickshank, one day after a transaction between him and Bramber Alternative (Pty) Ltd, a subsidiary of Fidentia to sell Ovation and Common Cents (Steenkamp 2007, p.21). After the curatorship of Fidentia, the FSB applied to the High Court to place Ovation and Ovation Nominees also under curatorship, as it was receiving funding from Fidentia (Peterson & Levin 2007, p.14).

The Ovation curators reported that various irregularities had been committed by Ovation's management, of which the most notable was Ovation's failure to perform reconciliations on its administration systems, a lack of proper corporate governance – and contraventions of legislation, the disastrous incorporation of its business into the operations of Fidentia – and attempts to transfer R370 million of clients' funds to Fidentia (Peterson & Levin 2007, p.12).

2.5.2 Fidentia Holdings

Messrs. JAW Brown and HR Bam joined Fidentia in January 2003, when at that stage they had as their only client, Mr SW Goodwin's company Worthytrade 185 (Pty) Ltd (Steenkamp 2007, p.13).

Fidentia Asset Management (Pty) Limited ("FAM"), an investment manager was bought by Fidentia in March 2003. Messrs. JPN de Jongh, JAW Brown and GA Maddock were the key individuals of FAM responsible for the oversight of the business. Mr Brown was also

the chairperson of Fidentia, while Mr Maddock was the audit partner of Maddock Incorporated the auditor of Fidentia and FAM (Steenkamp 2007, p.16).

From 2003, FAM secured larger investors, such as the Transport Education Training Authority ("TETA"). FAM promised TETA a return of up to 10.5% on their approximately R200 million that was invested. Fidentia also managed to get R1,2 billion of the Mineworkers Provident Funds beneficiary funds, which they transferred to the Living Hands (Pty) Ltd and the Living Hands Umbrella Trust (Steenkamp & Malan 2009, p.27).

After Mr Bam laid a complaint with the FSB, an inspection into the affairs of Fidentia and FAM was conducted; and on 1 February 2007, the High Court granted the FSB's application for the curatorship of Fidentia; while on 6 March 2007, Messrs. Brown and Madock were arrested on charges of theft and fraud (Steenkamp & Malan 2009, p.27).

Steenkamp and Malan (2009, p.28) explains that the failure of Fidentia may mainly be attributed to the non-existence and total disrespect of corporate governance principles. Mr Brown, as the CEO and Chairman of Fidentia, had unlimited powers, and with his autocratic management style was never even questioned. Mr Brown disregarded his fiduciary responsibilities, as he for instance, registered properties in his family trust's name and utilised company property for his own exclusive lifestyle – without paying any rent.

FAM did not keep proper accounting records, and FSB's inspectors found that R689 million of client's assets could not be accounted for, while clients' funds were utilised to pay for business expenses and the acquisition of several companies in the Fidentia Group. FAM disguised the nature of the investment held on behalf of clients – and allegedly inflated the value of clients' assets. FAM allegedly sent out incorrect statements to clients. There was apparently no risk management within Fidentia (Steenkamp & Malan 2009, p.28).

From the above discussions as a background to the discussion on fraud it becomes evident that there are different viewpoints on the definition of fraud, and an array of types of fraud. For the purpose of this study, investment fraud will now be defined.

2.6 CONCLUSION

As stated in **Chapter 1,** the study will not include investment fraud relating to market manipulation or insider trading. In terms of the Securities Services Act (36/2004), the Directorate of Market Abuse of the FSB must investigate these abuses. Although investment managers must have internal controls in place to ensure that their employees do not manipulate the market or commit insider trading, this does not fall within the ambit of the supervision of investment managers, in terms of the FAIS Act (37/2002).

Investment managers should be trusted by their clients (investors), and any misrepresentation or injustice to clients by the investment managers should be investigated, once it becomes known. As may be seen from the cases described in **paragraph 2.4** above, clients entrusted their funds to an external party that had the duty of caring for their interests. The persons in control of the companies, however, violated the trust and misappropriated the funds – and then misrepresented to their clients – through false reporting that their funds were still intact.

As described in **paragraph 2.3** above, investment fraud is similar to management fraud, as it is committed by persons in positions of trust who can manipulate internal controls to falsely misrepresent the financial results of an entity (management fraud) or falsify the off-balance sheet investments of a client (investment fraud). This misrepresentation is normally done to hide the fact that the investments are lost or do not exist – or because the management wants to increase its own wealth by charging higher performance fees on performance that does not even exist.

For the purpose of this study, investment fraud is defined as the intentional misrepresentation made by investment managers relating to investments entrusted to them by their clients (investors) that causes actual or potential prejudice to the client.

Investment fraud can originate in two ways: *Firstly*, schemes that are started with fraudulent intent; and *secondly*, schemes where there are unrealistic expectations by investors, or a change in market conditions that leads the investment manager to hide the losses from investors – through fraudulent communication (Ganshaw 2010, p.207).

Investment fraud scandals, such as that of Madoff (refer to **paragraph 2.4.4** above), in the financial services industry have prompted debate about how financial institutions should be regulated (Gadinis 2008, p.1). In the next chapter, the supervision and regulation of investment managers will be discussed.

CHAPTER 3:
THE SUPERVISION OF INVESTMENT MANAGERS

3.1 INTRODUCTION

Investment fraud is a broad concept and this study will only concentrate on schemes devised by investment managers. Investment managers operate in a regulated environment and must have a licence to conduct business as a financial institution (FAIS Act 37/2002, sec.7).

When describing the external oversight of financial institutions, the terms regulation, monitoring and supervision are used interchangeably. Goodhart *et al.* (1998, p.189) define supervision as the "*more general oversight*" of financial institutions' behaviour; regulation as, the "*establishment of rules of behaviour*"; and monitoring as, "*observing whether the rules are obeyed*".

The supervision and regulation of financial institutions is "*necessary to help manage the risks and vulnerabilities, protect market integrity, and provide incentives for strong risk management and good governance of financial institutions*" (World Bank & IMF 2005, p.5). Good practices in the supervision and regulation of investment managers (market intermediaries) are reflected in the international standards set by IOSCO (World Bank & IMF 2005, p.142).

The three core objectives of IOSCO are the protection of investors, ensuring that securities markets are fair; that they operate efficiently and are transparent, and reducing systemic risk (IOSCO 2010, p.3).

The regulation of investment managers aims to ensure that they conduct their business with their clients with due care and diligence. The regulation of investment managers consists of licensing requirements and market conduct rules imposed by the regulator (Carvajal & Elliott 2007, p.26). The regulation is therefore generally referred to as market conduct regulation.

In this chapter, the concepts of market conduct regulation, supervision and the monitoring of investment managers are *firstly* discussed – to provide the reader with the context of regulatory oversight. *Secondly*, the extent of regulation and the supervision of investment managers in South Africa are provided. *Thirdly*, a comparison is made between the South African supervision methodologies and those of the SEC in the USA and the FSA in the UK. *Lastly*, a conclusion is drawn on whether, in terms of its mandate, the FSB can adapt its processes and methodology to apply a fraud auditing approach to proactively identify any possible investment fraud.

3.2 MARKET CONDUCT REGULATION

The main purposes for the supervision and regulation of investment managers are investor protection (Allen & Herring 2001, p.1). Solaiman (2009, p.305) describes securities regulation as "*the protection of investors from corporate misfeasance".* As such, the regulation relies heavily on disclosure – to ensure that investors make informed decisions (Solaiman 2009, p.306). Investors are not always sufficiently sophisticated to evaluate the quality of the information disclosed to them (Allen & Herring 2001, p.8). Some investors do not always act wisely; they are naive and are easily fooled or misled; and as such, the regulation of investment managers will not always prevent or remove the possibility of wrongdoing by the manager (Solaiman 2009, p.306).

One of the reasons for the vulnerability of investors is that it is difficult to determine whether unfavourable investments returns can be attributed to wrong investment decisions due to the inherent unpredictability of the securities market, or whether they are due to the investment manager's incompetence or dishonesty (Allen & Herring 2001, p.8).

Goodhart *et al.* (1998, p.6) state that contrary to prudential regulation, that ensures the safety and soundness of institutions, market conduct regulations establish rules and guidelines on the appropriate behaviour and business practices of institutions when dealing with clients. In the financial services industry, the problem with consumer protection is greater than it is in other professions, mainly because of the principal-agent conflicts that exist and the handling of clients' money. These issues make fraud more likely (Goodhart *et al.* 1998, p.6).

Allen and Herring (2001, p.8) identify the incorrect choice of a client who selects incompetent or dishonest investment managers, and the "*moral hazard*" of the managers who put their own interests above those of the investor, or the blatant committing of fraud as the two reasons why market conduct regulation has become necessary.

One of the main reasons for regulation in financial services is to monitor (supervise) the fiduciary role in the principal-agent relationship (Goodhart *et al.* 1998, p.6). The regulator therefore establishes "fit and proper" requirements for investment managers, prior to licensing. After licensing, the investment managers must comply with the conduct of business rules; and the regulator must apply criminal sanctions for any contravention of these rules, in order to deter wrongdoing, and to ensure that there are adequate incentives in place to treat customers fairly (Allen & Herring 2001, p.9).

The efficient operation of the financial markets depends on the public's confidence that the investment managers who intermediate in these markets operate according to rules that are fair, transparent and place the interests of the client first (Allen & Herring 2001, p.11). Regulators supply regulatory services which are seen as a public good demanded by consumers (Allen & Herring 2001, p.11). But as regulation is not supplied through a market process, the consumer is not able to indicate what type of regulation is required, or the price they are prepared to pay to create a trade-off between costs and benefits (Goodhart *et al.* 1998, p.62).

Consequently, regulatory lapses and failures constitute a necessary trade-off between the cost and the benefits of regulation – as the degree of regulation that would remove all possibility of failure would be excessively high and would outweigh any benefits to the consumer (Goodhart et al. 1998, p.65).

Unethical managers may be able to benefit from the reputation established by ethical managers and take advantage of unsophisticated clients to increase their own profits. The underlying principle for market conduct and conflict of interest rules is to rectify this malicious incentive for unscrupulous managers (Allen & Herring 2001, p.9).

The moral hazard of regulation is described as the danger that the implicit contract is created by the regulator who establishes regulatory requirements and the consumer of

such financial services. The consumers assume that the regulatory environment makes it safe for them to deal with financial institutions, and that less care is necessary to protect the client (Goodhart et al. 1998, p.15). Clients of investment managers *"need to recognise that regulation and supervision do not protect them against all possibilities of loss*" (Goodhart *et al.* 1998, p.15).

Goodhart *et al.* (1998, p.39) comment on the failure in Barings Bank Plc and state that the reaction was that supervision needed to be increased; but on closer inspection of the facts, it became evident that the failure was not that of inadequate regulation, but poor internal monitoring of internal controls. The external regulation to prevent such cases of fraud would have had to be pervasive, intrusive and expensive as to be practically impossible of implementation.

Goodhart *et al.* (1998, pp.39-42) identifies three risks to regulators. *Firstly*, the complexity and speed with which regulation needs to adjust to new innovations in the financial markets make general external rules difficult to enforce. As such, regulators focus on reinforcement and the monitoring of internal mechanisms of management oversight and control. This in itself creates problems, as managers have self-interest which does not correlate with the regulators' objectives. *Secondly*, the globalization trend makes it difficult for regulators to act within their national laws and regulations, while financial institutions operate globally under different jurisdictions. *Thirdly*, internal risk-management frameworks are reliant on human interface of management that can manipulate these processes to their advantage.

The business of investment managers, therefore, presents a greater probability for fraud – and it should be closely supervised. Due to the nature of the investment business, individual clients do not have any incentive or opportunity to monitor the managers closely. This then provides a good reason for investment managers to be regulated (Allen & Herring 2001, p.24).

Market conduct rules applicable to investment managers play an important role in reducing the opportunities for abuse by investment managers; thereby, increasing the willingness of investors to participate in the financial markets (Allen & Herring 2001, p.26).

Regulators should have effective enforcement of financial regulation. Enforcement refers to the ability of the regulator to ensure compliance with the regulations through active supervision, and to bring legal action against financial institutions that do not comply or violate the rules (Carvajal & Elliott 2007, p.11). To be an effective regulator, the regulator must be able to obtain information from investment managers in a well-timed manner in the course of supervision. Regulators must be able to impose sanctions in the form of penalties against investment managers who do not comply with the rules (Carvajal & Elliott 2007, p.19).

Firm enforcement of market conduct rules provides investment managers with the motivation to adopt procedures that ensure that clients are treated fairly, and that their employees conduct themselves properly to maintain the managers' reputation (Allen & Herring 2001, p.9).

The main problem associated with the ineffectiveness of enforcement relates to the capacity of the regulator to implement adequate supervisory programmes and to correctly use the enforcement powers. Staff with the ability to conduct supervisory and enforcement actions are important to the success of supervision of investment managers (Carvajal & Elliott 2007, p.19).

3.3 THE SUPERVISION OF INVESTMENT MANAGERS

The regulation of investment mangers mainly exists to protect clients' assets from the insolvency of the manager, or misappropriation by the manager or the employees; and, to ensure that managers are fair and diligent in dealing with their clients. Regulation aims to set licensing criteria (ensure only persons with sufficient resources and qualifications and integrity can enter the industry), prudential standards (ensure there is investor protection against unexpected financial failure of the manager), internal controls and risk management standards and business conduct rules - ensuring that clients are treated fairly (Carvajal & Elliott 2007).

The FAIS Act (2002, sec.8) requires that all investment managers be licensed. A set of criteria termed "the Fit and Proper Requirements" has been set. This deals *firstly*, with the

honesty, integrity and competency of management, as well as employees involved in the rendering of financial services (management of assets). *Secondly*, the requirements set out the minimum operational ability of the regulated entity and its management in overseeing the rendering of the services and the solvency requirements of the regulated entity (Millard & Hattingh 2010, pp.33-35).

Investment managers must after licensing ensure that they can comply with an array of requirements, the most notable of which is the compliance with the codes of conduct provided for in section 16 of the FAIS Act (37/2002). The general code deals with requirements, such as the specific duties of due skill, care and diligence in the interests of the client, avoidance of conflicts of interest, confidentiality and disclosure, while the specific code applicable to investment managers deals with suitability analysis before entering into a relationship with the client, any mandate with the clients, the management of clients' funds, prohibitions in the management and reporting to clients (Millard & Hattingh 2010, pp.116-136).

The FSB, as the regulator, has the power to conduct onsite visits and inspections of investment managers, to determine whether they comply with the requirements set out above (FAIS Act 37/2002, sec.4).

In assessments conducted by the IMF, they identified a lack of trained regulatory staff to oversee investment managers effectively. The conditions are ineffectual in many other countries. This mainly led to the ineffective execution of the regulators' supervisory functions, such as onsite inspections programmes and reporting to the regulator, or not generating the desired results (Carvajal & Elliott 2007, p.19).

IOSCO (2010, p.6) prescribes in its principles that a regulator should have comprehensive inspection, investigation, surveillance and enforcement powers. These powers must be effectively implemented in conjunction with an effective compliance programme. The principles do not provide details relating to how the inspections and investigations must be conducted and what comprises an effective compliance programme.

Llewellyn (2006, p.7) identifies the limitations on supervisory resources and the high cost, as being some of the common challenges that regulators face. Therefore, regulators focus

on a risk-based supervisory approach in allocating their resources to financial institutions they regard as being the most risky (Llewellyn 2006, p.8).

Risk-based supervision is a structured approach that the regulator follows in the processes of licensing and supervising institutions. Here, the risk that the entity poses to regulatory objectives is identified as soon as possible; it is prioritised and mitigated. The objective of risk-based supervision is to assess the soundness of regulatory institutions and intervene on a timely basis, where the practices of institutions are seen to be imprudent (Stewart 2005, p.43).

The risk-based supervision focuses on deciding what the probability and impact factors are, and on choosing the regulatory responses, the development of regulatory tools – and then assigning the limited resources to concentrate on high risk areas (Hutter 2005, p.7). One of the regulatory tools that can be used is onsite visits to an entity's business.

3.4 REGULATORY ONSITE VISITS

IOSCO's (2010) sixth principle requires regulators to have a process to monitor, and to mitigate and manage systemic risk. Monitoring will mean that regulators must observe whether investment managers obey the market conduct rules (Goodhart *et al.* 1998, p.65). In the past decade, financial regulators have moved – for various reasons – to a risk-based approach in supervising financial institutions (Black 2004, p.4). Although risk-based supervision is applied differently by different financial regulators, the core principles remain basically the same. A short summary of the emphasis that, for instance, the FSA in UK and the SEC in USA, place on risk-based supervision in their onsite visit (inspection) programme will now be discussed.

3.4.1 The risk-based supervision approach of FSA

The FSA's risk-based approach to regulation is called the Advanced, Risk-Responsive, Operating framework ("ARROW"). With ARROW, they assess the impact which, in turn, determines which one of their four approaches will be used. The impact is determined by the financial institutions' industry sector. Depending on the impact, various methodologies are used to determine the probability that the institutions will cause the FSA to not meet its

statutory objectives, namely: maintaining market confidence, consumer protection, promoting the public awareness and reducing the incidence of financial crime. Probability is calculated in terms of the inherent risks an institution takes in terms of its business model and the controls that are in place relating to the risks (FSA 2006b, pp.5-9).

A central part of the ARROW assessment is done through onsite visits to the financial institutions which the FSA regulates (FSA 2006b, p.10).

For higher impact institutions, a full ARROW risk assessment of probability (all business risks and control risks) will be performed. The FSA's onsite teams have full discretion on the areas and issues they want to include in the scope of their assessment (FSA 2006a, p.18).

The process that is followed may be summarised as follows, namely: planning is conducted through an evaluation of the documentation obtained from the institution. The planning stage is followed by an onsite visit to the institution, during which any gaps in the information in possession of the FSA are filled in, and specific areas of the business are investigated. The visits normally consist of a number of interviews with the key personnel of the institutions (FSA 2006a, p.26).

After the planning process, the team will do a probability assessment and prepare a Risk Mitigation Plan for the institution. This is vetted through the FSA's internal peer review processes. The institutions management is then given two weeks to comment on the draft plan – by correcting any factual errors and suggesting any alternative ways to get the desired outcomes identified in the plan. A final letter and plan is then sent to the intuition's board of directors. The institution must then put a plan in place to ensure that it can carry out the steps agreed on in the plan and assign personnel to be held responsible for the different areas identified (FSA 2006b, p.10).

Although the FSA's main objective with onsite visits is not to detect fraud, they do include an evaluation of the institution's anti-fraud programmes and culture, senior management's role in establishing the culture in the systems, and the controls in their risk assessment. It focuses its efforts on specific frauds (Robinson 2007).

3.4.2 Examinations by the SEC's Office of Compliance Inspections and Examinations (OCIE)

The SEC's mandate, *inter alia,* includes enforcement of the securities law, by detecting problems in the securities markets, monitoring the compliance with securities laws, alerting investors to any contravention, taking action against wrongdoers – and returning funds to harmed investors, as well as ensuring that investors receive complete, accurate and transparent information on making informed decisions (Rezaee & Riley 2010, p.263).

Due to resource constraints, the OCIE focuses its resources on the financial institutions where investors and market integrity are most at risk. It aims to proactively detect and deal with potential areas of compliance risk, to detect fraud, to conduct inspections and examinations – and also to take any necessary steps to remedy identified problems (SEC 2010, p.3). The OCIE identifies risk and prioritises risks in its risk-assessment process, through the analysis of internal information and the allocation of resources to specific areas where further regulatory or examination attention is needed (SEC 2010, p.2).

The main objective of the OCIE's examinations is to test the financial institutions compliance with securities laws and regulations. The examinations mostly include onsite visits to the financial institutions premises, but can also include off-site work (SEC 2010, p.12). The examinations focus on risks; and where the examination was initiated as the result of some specific risk identified, greater focus will be placed on those risks. Others in the personnel may obtain a general understanding of the entity's compliance and internal control environment, and identify any risks in the financial institution that require attention (SEC 2010, p.13).

The examination process that is followed may be summarised as follows:

Advance preparation is done for an examination. This includes research in Self-Regulatory Organisation's records and other data bases, a review of the institution's statutory reports that have been submitted, together with a plan of the risk areas that need to be reviewed. The institution will normally receive a list of records that need to be available during the onsite meeting. During the visit, the inspection team reviews the books and records of regulated entities (this takes up most of time), interviews management and the firm's

employees, and analyzes the entity's operations. The team will have questions, while they review the books and records. The firm will designate a person to answer the questions of the onsite visiting team. Such a person must be available. OCIE expect that the employees of the financial institution are candid when answering questions – to avoid creating the impression that the institution has something to hide (SEC 2010, p.15).

An exit interview is normally conducted to discuss the deficiencies identified and to reach an agreement on any outstanding documentation, and the timelines reached for submitting such (SEC 2010, pp.16-17). The examination work continues after the visit, and as such, the team consults internally, and where necessary, may even obtain legal and accounting opinions to ensure consistency. The preliminary findings of an institution's examination may be compared to similar institutions to ensure consistency (SEC 2010, p.17).

The end result of an examination depends on the findings, and is normally a deficiency letter that is issued to the institution. If serious issues are identified, the matter is referred to the Enforcement Division of the SEC (SEC 2010, pp.17-18).

Before finalising the letter, the team will contact the institution and conduct an exit conference – where the deficiencies and appropriate corrective actions will be brought to their attention – and the institution will have the opportunity to provide additional documentation or information. The deficiency letter is then issued to the institution. The institutions must then inform the SEC in regard to the corrective actions that will be taken to remedy these deficiencies (SEC 2010, p.18).

The OCIE focuses on those areas where the focus is on investment managers' activities (SEC 2010, p.19). They check that the clients' investments portfolios are priced correctly and that the manager has effective policies and procedures for determining the value of portfolio holdings and calculating the net asset value. Checks are done to ensure that the manager reports to the clients periodically, and that the reporting is preferably done by a third party. They ensure that client information is protected from any unauthorized access and destruction in terms of the manager's business continuity plan. Investment management decisions must be consistent with the clients' mandates with reference to the client's investment objectives and restrictions. When managers make use of complex

investment products – and in the case of the management of money market funds – a more detailed scrutiny is done. The effectiveness of policies and procedures for safeguarding clients' assets from theft, loss and misuse must be evaluated. The institution's compliance culture and compliance framework, including monitoring conducted, must be tested; and any overriding of the controls by management or other persons in control of the investment manager, are also tested.

Tests are done to ensure that orders are placed in ways that result in best execution practices (SEC 2010, pp.19-22).

Emphasis is placed on the evaluation of the codes of ethics of the manager, and how such codes are designed to prevent market abuse through front-running, insider trading and market timing by traders in their personal accounts. Policies and procedures relating to ensure the accuracy of performance claims, advertisements, and other marketing materials and the effective disclosure of conflicts of interest must also be scrutinised (SEC 2010, pp.19-22).

In 2009, the OCIE changed its examination programme and are now placing more emphasis on fraud detection (SEC 2010, p.2).

These international regulators have their policies and procedure to examine and proactively detect and deal with any potential areas of compliance risk, to detect fraud, to conduct inspections and examinations, and to take any necessary steps to remedy identified problems. In South Africa, the FSB fulfils this task, and it has its own objectives, policies and procedures for examining and detecting fraud.

3.4.3 FSB's Onsite visits to investment managers in terms of the FAIS Act

In South Africa, all investment managers must be authorised in terms of the FAIS Act (37/2002, sec.7) as discretionary financial service providers. Investment managers are organisations that fall within the definition of a financial institution in terms of the FSB Act/2002. Investment managers manage financial products (securities such as shares,

bonds, debentures etc.) on behalf of their clients (investors) and in terms of an agreed mandate to meet specified investment goals (Millard & Hattingh 2010, p.34 & 133).

Regulatory onsite visits are performed in terms of section 4 of the FAIS Act (37/2002) to discretionary financial services providers (investment managers) by the employees of the FSB. In terms of section 4 of the FAIS Act (37/2002), the FSB as the regulator has been afforded the power to conduct onsite visits to determine an investment manager's compliance with the FAIS Act. These powers include the entry of the offices of investment managers at any time during business hours, the request for any documentation, the examination and copying of the documentation, and the request for any information and an explanation of information or documentation provided.

These visits form part of the FSB's risk-based supervision methodology in supervising investment managers (Millard & Hattingh 2010, pp.156-158). Onsite visits entail a detailed review of the investment manager's business, in order to determine compliance with the FAIS Act/2002. The following aspects, inter alia, are considered.

The onsite team obtains an understanding of the individual investment manager's organisational structure, the nature of its business and its strategy, the Enterprise Risk Management Framework, and the policies, procedures and internal controls. An overview of the management's experience, the allocation of management's responsibility, the corporate governance structures that exist, the human resource function, together with the level of compliance and the business culture are evaluated. A review of the interaction of the investment manager with clients and the compliance with the code of conduct is done (FSB 2009a).

The examination process that is followed may be summarised as follows (Millard & Hattingh 2010, pp.156-158). A suitable time will be agreed upon with the investment manager for conducting the onsite visit, and the manager will be requested to send specific information to the FSB. The onsite visiting team will then analyse the information and send confirmation to the manager on who they would like to interview during the visit and any additional information and documentation that must be available during the visit. At the onsite visit, the onsite team will conduct interviews with key members of staff of the manager and scrutinise all the relevant documentation.

The visit ends off with an exit interview, during which preliminary findings are discussed and an agreement is reached on the timelines for submitting any outstanding information to the onsite visiting team. The outcome of the visit is a risk-mitigation plan which highlights risk areas and any areas of non-compliance with the legislation. The plan is sent to the manager. He/she must undertake to take any corrective actions to mitigate the risks or correct any areas of non-compliance.

Similar to the approached followed by the FSA, the FSB does not specifically, as in the case of the SEC, search for fraud as part of its onsite visit objectives and methodology. Fraud detection will, therefore, only take place should it be stumbled on during the assessment of the different risks within the regulated entity or where complaints are received from clients.

3.5 CONCLUSION

Investment managers, in terms of a written agreement (mandate), obtain discretion over a client's funds, and as such, are empowered to deal with these funds within specific limitations and restrictions. They, therefore, owe their clients a high degree of conscientious care when managing the funds. Should the duty of care be neglected or disregarded, this could lead to investment frauds, as described in **Chapter 2**.

As stated above, the FSB has a mandate to protect the consumer; and this will include ensuring that the financial institutions they license act lawfully. The objective of the FAIS Act (37/2002) is consumer protection and the professionalizing of the financial services industry (FSB 2008, p.24). To protect investors, there is an underlying principle that the regulator should have adequate regulation and supervision in place to detect any possible fraud. Investors and the regulator alike can never have a 100% guarantee that all institutions will at all times act honestly.

As such the FSB's mandate can indirectly be interpreted as giving it the obligation to detect and deal with fraud which they may disclose in the course of their regular duties. It is not as direct as the mandate of the FSA and SEC where specific obligations to combat fraud is incorporated in the regulators mandates.

From the above analysis on the different methodologies used by regulators, it can be surmised that the methodologies are similar. The processes differ in the different jurisdictions, but the end result to supervise the managers of investment funds remains consistent.

This process is based on three basic steps. The analysis of information and documentation at the disposal of the regulator, interviews of key staff of the manager and scrutiny of the manager's internal controls and risk-management processes. In the USA, more emphasis is placed on the detection of fraud, while the FSA and FSB place their emphasis on the companies' risk-management processes. The FSB should consider adapting its approach to place more emphasis on fraud pro-active fraud detection.

Limited information is available on the specific techniques used during these onsite visits, but if the broad principle of risk assessment is compared with the work done in other oversight functions, such as internal and external auditing, it appears to be comparable.

Proactive fraud auditing techniques can form part of the regulator's supervisory process. Such steps would assist the regulator in the detection of fraud. In the next chapter, fraud auditing will be discussed and how it can be adapted to the regulatory methodologies.

CHAPTER 4:
THE USE OF A FRAUD AUDITING APPROACH

4.1 INTRODUCTION

In **Chapter 2**, investment fraud for the purpose of this study, was defined as the intentional misrepresentation made by investment managers relating to investments entrusted to them by their clients (investors) that causes actual or potential prejudice to the client.

The examples that are discussed in **Chapter 2** gives some insight into how investment managers have in recent years deceived investors in investing into fraudulent investment schemes. It is important to consider how investment fraud committed by investment managers could have been avoided by the various role-players responsible for the oversight of investment managers. Wells (1997, p.426) remarked that "*a statement of financial health is all the naive investor requires before handing millions of dollars to well-tailored con artists*". It is therefore important that the regulator be alert to the possibility of investment fraud when introducing supervisory programmes.

Although fraud investigations by regulators have increased in intensity over the past few years, most of these investigations were carried out after the occurrence of fraud had already become known (Coburn 2006, p.348).

As stated in **Chapter 1,** there is not a great deal of research that has been done on the detection of investment fraud. Investment fraud does, however, resemble some of the characteristics of management fraud, and as such, a fraud auditing approach in relation to management fraud will be discussed and then applied to investor fraud.

In this chapter, a fraud auditing approach will be discussed, together with its relevance for the regulator's supervisory approach to investment managers. These issues will, *inter alia*, be considered. To understand the concept of fraud auditing it is *first* necessary to explore the processes of governance that need to be in place, as well as the role-players involved in the prevention and detection of fraud. *Secondly,* one needs to understand the driving forces that lead people to commit fraud.

4.2 COPORATE GOVERNANCE STRUCTURES APPLICABLE TO THE PREVENTION AND DETECTION OF FRAUD

Corporate governance consists of external and internal mechanisms designed to align the interests of management with those of the shareholders, and ensure compliance with the applicable laws. The corporate governance aim is to improve investor confidence, while focusing on ownership structure, the legal system and capital markets (Rezaee & Riley 2010, p.125).

The ACFE (2010, p.5) in its 2010 report to the Nations, indicated that external audit is the most widely recognised control mechanism to prevent fraud.

In terms of the regulation of investment managers' financial statements are subject to financial audits (FAIS Act 37/2002). The auditor is required to – in cases where clients' funds are kept in safe custody – to perform additional procedures, and to issue a limited assurance report on the separate account a manager must keep in which to deposit clients' funds (FAIS Act 37/2002, sec.19). Financial audits focus on providing reasonable assurance that financial statements do not contain material misstatements.

The focus on finding fraud is limited, and only requires the auditor to access fraud risk and apply professional scepticism, when considering management representation and audit findings (IFAC 2010, pp.12-14; Singleton *et al.* 2006, p.4). Financial audits are, therefore, not the best tool for detecting fraud (ACFE 2010, p.5).

Investment managers must, as stated in **Chapter 3,** have internal controls in place to ensure they limit the risk that clients will suffer losses through fraud or other dishonest acts (FAIS Act 37/2002, sec.15).

Finding fraud is not easy – especially for external or internal parties who are not part of the day-to-day management and oversight of an organisation. The ACFE (2010, p.16) indicates that the most common detection method of fraud, since 2002, is whistle blowing (40.2%), followed by management review (15%), internal auditors (14%), and external auditors (4.6%). They also note in their report that 11% of fraud cases are identified by channels outside the anti-fraud control structure.

Fraud can, however, be reduced through effective corporate governance that focuses on both the prevention and the deterrence of fraud (Coburn 2006, p.349). The global financial crises in the past decade have highlighted specific concerns relating to corporate governance (Coburn 2006, p.349).

The King III Code on Corporate Governance requires South African companies to – in terms of its risk assessment – also consider fraud risk. This will require audit committees to review whistle-blowing arrangements, and to conduct appropriate investigations relating to such reports. In addition, the audit committee should also consider matters that may result in material misstatements in the financial statements due to fraud (Institute of Directors 2009, pp.68-69).

Management fraud is normally committed by senior management, and if it involves management overriding of the controls and collusion, this would make it difficult to detect (Singleton *et al*. 2006, p.64). It is therefore, important to have effective governance structures within companies, as they can prevent and detect management fraud (Rezaee 2002, p.10). Important contributors to facilitating management fraud are the ineffectiveness of a board of directors and its committees (Rezaee 2002, p.17). ISA 240 states that the primary responsibility for oversight to ensure fraud is prevented and detected is persons who are held responsible for the oversight over an entity (IFAC 2010, p.155).

Financial statement audits are effective tools in reducing the likelihood of management fraud occurring (Rezaee 2002, p.17). ISA 315 recommends that the auditor do a risk assessment of the organisation, and identify risk caused by material misstatements in the financial statements – leading to the danger of fraud (IFAC 2010, p.160). Part of the risk assessment should include that the engagement team responsible for the audit have a discussion in which the emphasis is placed on the possibility of management fraud being committed – even if they have no reason to doubt the management's honesty and integrity (IFAC 2010, p.160). To identify possible fraud it is important to understand what drives people to commit fraud.

4.3 WHAT DRIVES PEOPLE TO COMMIT FRAUD?

There is no single reason behind fraud; various factors must be taken into account, such as motivation, opportunities, technical ability, risk of discovery and its consequences (Singleton *et al*. 2006, p.8). Donald Cressey, who did research on the reasons embezzlers, whom he called "trust violators", committed fraud came up with the "Fraud Triangle" that consists of three legs, namely: pressure, opportunity and rationalisation (Wells 2008, p.13).

In the "Fraud Triangle", there is an interrelationship between the three driving forces (opportunity, pressure and rationalisation). These drive people to commit fraud (Wells 1997, p.20).

An opportunity to commit fraud exists in an organisation if employees believe that they can override anti-fraud controls. As such, fraud is mostly present when there is a lack in internal controls, or no management oversight, or the relaxation of controls (Singleton *et al*. 2006, p.11).

Persons committing fraud normally rationalise their actions, because they want to justify to themselves the circumstance that they are in that lead to them committing fraud (Wells 1997, p.18). Rationalisation is a conscious decision, as the perpetrators put their needs above those of others (Vona 2008, p.7). According to Cressey's study (in Wells 2008, p.18), rationalisation is linked to the "trust violator's" position and manner in which they commit the violations. He identified three types, namely: independent businessmen, long-term violators and absconders.

In terms of the characteristics of independent businessmen, it is relevant to note that where there were normally "covert deposits" entrusted to them, to have two common excuses. *Firstly,* that they were just "borrowing" the money entrusted to them; and *secondly,* that the funds were really their own funds (Wells 2008, p.18).

In an environment where there is sufficient pressure**,** even honest employees can commit fraud. Consequently, the opportunities for fraud must be minimised – by the introduction of anti-fraud programmes (Singleton *et al*. 2006, p.9).

When conducting a fraud audit the three elements of the fraud triangle must be measured, in order to understand how the fraud condition can lead to the likelihood of fraud (Vona 2008, p.8).

4.4 FRAUD AUDITING

Fraud auditors are actively involved in the prevention and detection of fraud (Singleton *et al*. 2006, p.44). Fraud auditing is different from financial auditing, and it involves a specific approach and methodology to identify fraud and search for the evidence thereof (Singleton *et al*. 2006, p.4). ISA 240 limits the objective of financial statement audits to the expressing of an opinion on whether the financial statements of entities are prepared in accordance with an applicable financial reporting framework (IFAC 2010, p.365).

This requires the auditor to apply professional scepticism, since fraud could exist whenever misstatements in financial statements occur. The auditor would then be required to perform procedures to identify the risks of material misstatement due to fraud; and to evaluate the entity's controls relating to the risk areas, in order to determine whether such measures had been implemented (IFAC 2010, p.365).

ISA 240 limits the types of fraud that are relevant to financial statement audits to the misstatements resulting from the misappropriation of assets and fraudulent financial reporting (IFAC 2010, p.365).

Fraud auditing, on the other hand, does not test the existence of internal controls and does not rely on management representations, but it does affirm the authenticity of transactions (Vona 2008, p.27). It therefore requires a mindset similar to that of the perpetrator, in order to uncover the fraud scheme – and a methodological approach in order to accomplish this task (Singleton *et al*. 2006, p.62). The fraud auditor focuses on accounting irregularities and peculiarities, exceptions and patterns of misconduct – to focus on the substance of the transaction, and not as financial auditors, but instead on the audit trail and any material misstatements (Singleton *et al*. 2006, pp.61 - 63). Fraud auditors can come to the conclusion that there is no known evidence of fraud, and as

such, indirectly provide evidence of the fact that internal controls are effective. Or, a suspicious transaction may be identified, and thereby provide evidence of fraud (Vona 2008, p.28).

The fraud auditor's first aim is to establish whether any suspicious transaction is not due to accidental or human error, and then to investigate it further (Singleton *et al.* 2006, p.62).

Fraud auditing focuses on the internal environment and encourages the detection, prevention and correction of fraud (Singleton *et al*. 2006, p.56).

4.5 THE DIFFERENCE BETWEEN FRAUD AUDITING AND FRAUD INVESTIGATION

Tickner (2005, p.57) explains that in any fraud investigation, it is important to be aware of the fact that the dynamics of investigation exist in real time. The first step in an investigation is to determine whether there is enough evidence to lead a professionally trained individual to believe that fraud has occurred – or may yet occur. If not, then the investigator should follow the fraud-theory approach (Singleton *et al*. 2006, p.54).

To detect fraud, an investigator has to understand the specific frauds that can be perpetrated, and how these are committed. Fraud theory starts with the identification of the most-likely fraud scheme, and how such a fraud is usually committed (Singleton *et al*. 2006, p.125).

Though audits and investigations are similar, there is an important difference – such as the body of knowledge and the standards used. Audits are based on auditing standards, accounting principles, policies and procedures, while investigations are based on the rules of evidence, and criminal and civil procedures (Vona 2008, p.191).

Fraud auditing in turn, is intended to identify transactions that have unresolved red flags in a specific fraud scheme. Fraud investigations are intended to refute or substantiate the allegation of fraud identified during the fraud audit, and to provide evidence concerning the required act or law (Vona 2008, p.191). When conducting a fraud audit, the auditor should always be aware of the fact that the matter can lead to further investigation and

prosecution, and as such the fraud auditor should ensure that strict procedures are followed in the conduct of the fraud audit and any subsequent investigations, with seamless transitions between the two (Vona 2008, p.192).

As fraud investigations are aimed at proving a crime in a court of law, it is of the utmost importance that the fraud auditor does not compromise the evidence in any way. For instance, the last step in an investigation is to approach the suspect to ensure that the case is not compromised by obtaining a confession that will not stand up in a court of law. The fraud auditor should, therefore, always be wary of the thin line that exists between fraud audit and fraud investigation, and know when to switch over from a fraud auditing mode to an investigating mode, or when to hand a case to another person for further investigation (Singleton *et al*. 2006, p.53).

4.6 THE FRAUD AUDITING APPROACH

A fraud auditing approach is designed to search for a specific type of fraud scheme. As the main goal of fraud auditing is to offer an opinion on the existence of fraud in an organisation – and as such, the use of data mining on specific samples of data to identify whether there are similarities in the data that relates to specific fraud schemes. The audit procedures employed are, therefore, focused to "*pierce the concealment strategy*" by collecting evidence independently from the perpetrator of the scheme (Vona 2008, p.27).

Although the work performed by external auditors, as described in ISA 240, differs from that of the fraud auditor, the approaches are similar. They both require the assessment of different fraud risks. ISA 240 requires the auditor to do specific work relating to the possible risk of management fraud which would include the following. *Firstly*, the auditor must obtain representation from management. The representation should include their assessment of any fraud risk that can indicate that the financial statements might be materially misstated. It should further indicate the risk-management processes that are implemented to identify and respond to possible fraud risk. Management must comment on the reporting of fraud-risk assessments to governance structure and the anti-fraud programmes within the organisation to sensitise employees to fraud risk. *Secondly*, if the entity has independent governance structures, the auditor will assess whether those in charge of governance have oversight over the fraud-risk assessment process. The auditor

should also assess the internal controls that management have introduced to mitigate risk and their knowledge of actual or suspected fraud cases.

The auditor must use the information obtained to collaborate management representations on fraud risk. *Thirdly*, the auditor must evaluate unusual or unexpected relationships and consider how they might influence the entity's fraud-risk assessment. This will include relationships within revenue accounts, which could be an indication of management fraud. *Fourthly*, the auditor must consider any other information obtained that might indicate material misstatements in the financial statements because of fraud. *Lastly*, the auditor must evaluate other information obtained, and consider whether it indicates fraud risk factors that might be present (IFAC 2010, pp.160-161).

A fraud auditing approach will be discussed below. It is a similar approach to fraud risk assessment, as prescribed by ISA 240.

4.6.1 Identifying the intrinsically fraudulent scheme and any of its variations

The identification of the inherently or intrinsically fraudulent schemes and their possible variations is important, as one auditing procedure can detect an array of schemes or variations thereof, but the data mining for the variations may differ (Vona 2008, p.28). Different fraud schemes have different red flags (Singleton *et al*. 2006, p.125). Understanding the different fraud schemes that are possible, and are most likely to occur in a specific company, industry and operational environment assist in assessing fraud risk (Rezaee & Riley 2010, p.116).

For instance, management fraud is normally perpetrated by senior management for the benefit of the organisation and perpetrator, and as such, the red flags will be different from asset misappropriation (Singleton *et al*. 2006, p.129). Management fraud perpetrated as fraudulent financial reporting is divided in terms of ISA240 into six different categories – each with its own red flags. These include fictitious journal entries – to manipulate operating results, inappropriate adjustment assumptions, delaying or omitting revenue recognition in the financial statements, concealing or non-disclosure of the material facts,

engaging in complex transactions to misrepresent a financial position, or the performance or altering of records of significant or unusual transactions (IFAC 2010, p.168).

Like management fraud, investment fraud can also involve different types of fraud, as was discussed in **Chapter 2.** Investment fraud committed by hedge fund managers, such as the Madoff scheme, involves the making of promises to investors that a fund will yield high investment returns. When these promises cannot be met, client statements are falsified by, for instance, inflating the returns and paying out false returns to attract more investors (Sander 2009, p.224).

Fraud is committed by people, and as such, it is important to have an understanding of the likely persons that might commit a fraud scheme.

4.6.2 Fraud opportunities

Understanding who is more likely to commit fraud will help in identifying the perpetrators and will increase the auditors' awareness (Vona 2008, p.28). As explained above, in **paragraph 4.3**, the fraud triangle can assist in understanding what drives people to commit fraud, and as such to identify a red flag (Singleton *et al*. 2006, p.125).

Owners of internal controls are gatekeepers and determine what goes through and what does not; as such, they keep fraud out or let it in (Vona 2008, p.29). It is, therefore, important to understand who the owners of the internal controls are and how they link to the fraud scheme – to ensure any override of controls is seriously considered (Vona 2008, p.29).

As management fraud is normally committed by top management who are pressurised to meet financial targets that might be considered unrealistic (Singleton *et al*. 2006, p.131; IFAC 2010, p.167), it is easy for management to manipulate internal controls and coupled with collusion, this leads to significant management fraud (Rezaee & Riley 2010, p.117).

In most investment fraud schemes, as discussed in **Chapter 2,** it is evident that it is normally top management that has control to override controls who commit fraud. For

instance, in the case of Ovation, the CEO Mr Cruickshank, was able to divert clients' funds to his own personal accounts, while providing the staff of Ovation with fictitious returns (Peterson & Levin 2007, p.14).

4.6.3 The fraud scenario

When considering different scenarios, questions such as: Who would commit fraud? Where could such schemes occur? And how would it be perpetrated? - must all be considered. To develop the scenario, a good understanding of the internal control environment and procedures, the inherent business risks, the difference between control theory and reality, internal control inhibitors and fraud-concealment strategies must all be considered (Vona 2008, p.27).

The difference between control theory and reality is when, for instance, a manager must sign off on a specific transaction – to check that it is within policy (theory), but in reality the person just signs without checking, and as such, the control differs from its intention (Vona 2008, p.30).

Tickner (2010, p.8) indicates that there can be three systems in organisations, namely: the "*prescribed*" one, which is what is contained in the formal documentation and policies, the "*alleged*" one, which is how management perceive the system should work, and the "*actual*" one, which is what is applied in practice by management and employees. To find fraud, it is important to understand what is done in practice, and not what is contained in policy (Tickner 2010, p.9).

If there is no direct evidence of fraud, it is necessary to develop a fraud theory of different possible scenarios (Wells 2008, p.5). For instance, a common symptom that financial statement fraud exists is the ongoing deterioration of the quality and quantity of earnings, and as such, the fraud auditor should develop a theory of why deterioration took place. This is done by examining the nature of the transactions, for example, non-recurring transactions, long-term contracts, bill-and-hold transactions to establish the quality of earnings (Rezaee & Riley 2010, p.98). Brainstorming can be used to assist in the development of fraud theory and scenarios (Lynch 2006, p.1).

4.6.4 Building a data profile of the fraud scheme

To do effective data mining, it is important to build a profile of the data that can be used to prove that a fraud scheme exists (Vona 2008, p.32). For each of scenarios developed, specific data must be identified to build a profile. For instance, in the example of ongoing deterioration of the quality of earnings, the earnings of the past three years can be rebuilt and classified in terms of the type of transaction (Rezaee & Riley 2010, p.98).

Langevoort (2009, p.10) indicates that for the SEC to have revealed the Madoff scheme earlier, they should have verified returns and trades through verifying data in the possession of third parties, such as market counter parties and clearing firms which the Madoff scheme used. This would have enabled them to ascertain whether Madoff implemented the strategies he claimed to use in the management of his hedge fund. This was, however, never done – due to the vast number of data that had to be analysed (Langevoort 2009, p.11).

This indicates the necessity to develop data mining tools to be able search for specific investment fraud profiles.

4.6.5 Data mining to search for transaction data profile

Data mining is used to identify a discrete number of transactions that can be examined in terms of set fraud procedures. It is different from traditional audit sampling procedures, as it is biased towards specific errors (Vona 2008, p.32). Data mining can be used to judge fraud risk and exposures to fraud schemes by utilising quantitative routines to pinpoint potential fraud (Tickner 2010, p.388).

When applying data mining, both the internal and external data of any format can be used, but it is easier if it is in digital format, as specialised computer programmes can be used to do the analysis (Tickner 2010, p.388). Computer-assisted audit techniques (“CAATs”) can be used to efficiently automated audit of data (Kranacher, Rilley & Wells 2011, p.265). It is, however, important to remember that computer systems perform only as they are

programmed to, and as such, must resemble the business process (Singleton *et al*. 2006, p.155).

The data is tested against specific red flags; if the data do not show any disregard for policies or controls, then they are disregarded. If there is a disregard for policies or controls, the data are further examined to determine whether there is any error or fraud. The data should then be accumulated by different factors, depending on the red flag. The high occurrence of the different level of anomalies must then be examined and further investigated (Singleton & Singleton 2007, pp.148-149).

The analysis assists in the fraud auditing process, in order to identify potential transactions or documentation and then to do further auditing procedures (Singleton *et al*. 2006, p.151).

4.6.6 Fraud auditing procedures

Fraud auditing procedures are designed to determine the true nature of a business transaction and they do not test the existence of internal controls or rely on management representation. They do not assume that the transaction is false, but focus on the concealment strategy and the associated red flags of specific fraud scheme (Vona 2008, p.32).

Fraud auditing procedures would include document examination, economic substance procedures, independent data comparison, logical testing, trend analysis and fraud magnitude tests (Vona 2008, p.32).

Document examination takes place when examining documentation relating to specific types of fraud schemes to identify red flags (T. Singleton et al. 2006, p.64; Vona 2008, p.32). Economic substance procedures are performed to ensure that the transaction is authentic and whether assets indeed exist. Independent data comparisons comprise procedures that are used to compare the transaction with another database (electronic or paper file or interview) that is not under the control of any possible perpetrator (Vona 2008, p.32).

Logical testing is where a transaction is analysed – to ensure that it makes logical business sense. Trend analysis is used to determine whether the transaction pattern of an activity is consistent with the predictable pattern of similar activities. A fraud magnitude test is where an economic model to predict the monetary value of a transaction is consistent with the predictable monetary outcome (Vona 2008, p.32).

The design of fraud auditing procedures should take into account the evidence – to ensure that logical conclusions are reached regarding the scheme, and whether the allegations can be proved (Vona 2008, p.36).

4.6.7 Considering the evidence

In fraud audits there is an inherent assumption that fraudulent transactions will be concealed and documents might be falsified; internal controls might not function as intended, and as such, the perpetrator of the fraud has made false representations regarding the transaction. When designing auditing procedures the auditor must, therefore, consider the quality of the evidence, the availability and possibility of how auditors might be deceived through the acceptance of dubious auditing evidence (Vona 2008, p.33).

The goal of fraud auditing when gathering evidence is to obtain independent documents and to rightly interpret and understand the red flags of false documents (Singleton *et al.* 2006, p.66).

Vona (2008, p.33) describes the location of evidence as being “on- the books”, where the information is within the organisation and can be resolved by means of thorough document examination; or it may be described as, “off-the-books”, where a third party holds the records and the fraud auditor will require the assistance of third-party – or a confession from the person committing the fraud (Vona 2008, p.33).

4.6.8 Reaching a conclusion on the evidence of possible fraud

The goal of a fraud auditing procedure is to reach a conclusion on whether there is any evidence that the transaction is fraudulent, or there is sufficient and credible evidence that warrants a further investigation (Vona 2008, p.36).

Audit planning should always include information on whether a transaction is suspicious and warrants fraud investigation (Singleton *et al.* 2006, p.67). This helps the fraud auditor to ensure that a logical conclusion to the auditing process will be reached; and secondly, it is to ensure that any evidence would be admissible, should the fraud case be pursued. The identification of a suspicious transaction would clearly indicate the starting point of an investigation process (Vona 2008, p.36).

4.7 CONCLUSION

As described above, the fraud auditing approach is a systematic approach with different steps. These require, for instance, that specific data be extracted from the financial records (real data on the operational systems) to detect any possible management fraud (Singleton *et al*. 2006, p.160). The fraud auditing approach can assist in proactively identifying fraud schemes, by applying techniques – such as reasonableness and completeness tests, analysing trends and statistical analysis. These issues will be discussed in **Chapter 5** (Singleton *et al*. 2006, p.161).

In the detection of management fraud, the fraud auditor can consider various scenarios and analyse, for instance, the performance of a company, in order to identify possible fluctuations over time. These could possibly be red flags, indicating that there has been manipulation of the entity's performance.

The techniques above can also be applied in detecting possible investment fraud. Investment fraud can occur, for instance, where unrealistic expectations by investors – or a change in the market conditions – could lead the investment managers to hiding their losses from the investors, through the fraudulent communication of performance (Ganshaw 2010, p.207). Alternatively, the fraud scheme can be devised to show higher performance in investments, and to be able to take higher performance fees. Since these

fees are not really earned, could drain the client's assets over time. By applying a reasonableness and completeness test, and analysing the trends, the fraud auditor should be able to identify possible investment fraud scenarios. These would then need to be further investigated.

If compared with the processes used by regulators (as described in **Chapter 3, paragraph 3.4),** it becomes evident that approaches used by regulators in most instances are limited to utilising documentary and oral representations of management. These can be adapted to apply to the identification of inherently fraudulent schemes, considering different scenarios, fraud auditing procedures relating to document examination and economic substance procedures. With regard to data mining and fraud auditing procedures, such as logical testing and trend analysis, the regulator would have to obtain access to the operational systems of financial institutions.

As investment accounts kept by investment managers are off the balance sheet, and recorded in separate operational systems, it should be possible to clearly identify the relevant data. The adoption of a fraud auditing approach, together with specific techniques to detect investment fraud will be discussed further in **Chapter 5**.

CHAPTER 5:
THE APPLICABILITY OF A FRAUD AUDITING APPROACH TO DETECT INVESTMENT FRAUD SCHEMES

5.1 INTRODUCTION

This chapter will focus on the concealment strategies, red flags and audit techniques that form part of a fraud auditing approach, as discussed in **Chapter 4.** The techniques used to detect management fraud will be considered in this chapter and applied to investment fraud schemes.

Management fraud is caused by several factors that occur at the same time, and it mostly occurs when top management is under pressure to increase earnings. This type of fraud is simplified due to the subjective process involved in preparing financial statements, where a debit entry can, for instance, be either an expense or an asset (Wells 1997, p.426).

Financial statements are not perfect; and in terms of accounting principles, it does not need to be – as long as they are reasonable and fair. Not all mistakes are material, and as such, materiality is a user-oriented concept, but when many small amounts are added together, they can become material. Accounting principles require the matching of expenses and revenue during the same period. Fraud occur when management manipulates this concept – by declaring revenue too early and deferring expenses (Wells 1997, p.427).

Another important principle to ensure fair presentation in financial statements is consistency; and fraud can occur when consistency is intentionally disregarded, in order to increase profits (Wells 1997, p.428). Full disclosure of any and all material information that could affect the company's profits in the future must be disclosed, to ensure that the investor understands the implications of major events that might still occur (Wells 1997, p.430).

To be in an ideal position to detect fraud, a good understanding of an entity and the industry or environment in which it operates is necessary. This knowledge will assist in

better identifying certain red flags that indicate the possibility of fraud risk. These red flags can include, for instance, internal control weaknesses, nonsensical analytic relationships, unpredicted financial performance, unrealistic performance in comparison with competitors and transactions without any obvious business purpose (Golden *et al*. 2006, p.124).

5.2 FRAUD AUDITING PROCEDURES USED TO DETECT MANAGEMENT FRAUD

It is difficult to detect management fraud, as management is normally involved in these fraud schemes, and as such, can easily override internal controls (Wells 2008, p.337). Fraud detection techniques will never be able to detect all fraud, but the use of sound techniques can increase the likelihood that fraud will be discovered speedily. It is however, important to know where to look for evidence of fraud. This can be achieved by understanding the motivations of those committing fraud, and concentrating on financial accounts where fraud is more likely to occur (Ozmen 2009, p.6).

Various fraud auditing detection techniques can be used, such as financial statement analysis, unpredicted audit tests, observing and inspecting, making inquiries and conducting interviews (Golden *et al.* 2006, pp.121-122).

In the performance of fraud auditing procedures, it is important to have a specific attitude, in order to get the desired results. Professional scepticism must always be applied when evaluating information provided by management (IFAC 2010, p.159). Deceptions techniques must be considered, when reviewing documents. Applying the principle of trust with verification of information is important, as complacence on the honesty and integrity of management can so easily lead to the oversight of smaller misstatements that later evolve into large-scale frauds (Golden *et al*. 2006, p.122).

5.3 BRAINSTORMING

IFAC (2010, p.15) recommend that auditors have a discussion prior to conducting an audit to assess the exposure of financial statements to fraud with the engagement team. The discussion should allow for exchanging ideas on possible fraud scenarios; external factors that might create incentives, pressures or opportunities for management to commit fraud;

unexplained changes in behaviour of management or employees; and how "*element of unpredictability*" can be introduced in audit procedures. This process is commonly referred to as brainstorming (Bishop *et al.* 2007, p.22; IFAC 2010, p.15).

Several brainstorming techniques can be used such as paradigm-persevering (staying in current mindset) or paradigm-modifying (challenge assumptions and think outside of the box). Different approaches to brainstorming can also be use for instance face-to-face sessions where the individuals share ideas with open discussion or nominal brainstorming where individuals generate ideas and then come together to share it (Lynch 2006, p.2).

It is important that the brainstorming process is structured, an agenda is set, that team members are prepared and the team leader facilitates the session to ensure ideas are shared openly (Bishop *et al.* 2007, p.22). Beasley and Jenkins (2003, pp.3-5) identified the following drawbacks that can potentially influence the success of a brainstorming session. *Firstly*, group domination by one or two individual who take over the discussions and hinder the sharing of ideas. *Secondly*, the disengagement of part of the team from the process and where they leave the work to others in the group. *Thirdly*, "*Groupthink*" where the team members want to reach consensus and this leads to them not evaluating all ideas put forward. *Lastly*, "*Group shift*" where the team take extreme positions on fraud risk and thereby assuming fraud risk is high in all audits.

The brainstorming process is normally part of the planning process but it is also a good technique that can be used during the "wrap-up phase" to ensure that risks identified in the planning process were adequately addressed (Beasley & Jenkins 2003, p.11).

5.4 ANALYTICAL PROCEDURES USED IN THE DETECTION OF FRAUD

A common general detection method that is independent of a particular fraud scheme is the use of financial statement analyses (Singleton *et al*. 2006, p.130). Various analytical analyses methods, such as vertical, horizontal or ratio analysis can be used to detect fraud (Wells 2008, p.331). The overall objective of these analytical procedures is to identify the unexpected, such as relationships that do not make sense (Golden *et al*. 2006, p.365).

This is a useful tool in identifying any red flags that could indicate the possibility of fraud (Kranacher *et al.* 2011, p.438).

Analytical procedures are useful when there are thousands of transactions on which to focus the fraud investigation. The use of a variety of analyses in combination is normally necessary to corroborate the overall results of the various analytical procedures being performed (Golden *et al.* 2006, pp.365-366).

When using analytical procedures, it is important to have knowledge of the entity and the industry in which it operates, in order to ensure that proper comparisons between industry benchmarks can be made (Golden *et al*. 2006, p.371).

5.4.1 Financial statement analysis

The use of ratio analysis assists the users of financial statements to analyze the amounts in the statements in relation to each other and to major changes in the historical totals (Wells 1997, p.471). It can, in addition, be used to make comparisons between different business units in large organisations (Singleton *et al*. 2006, p.130), or to indicate changes in ratios from quarter to quarter (Coenen 2008, p.62). In fraud detection, the reason for the relationships and changes in amounts can indicate important information, as they can indicate red flags that would assist in directing the examiner to find any possible fraud (Kranacher *et al.* 2011, p.438).

If any misstatements in the accounts occur and are large enough, they would indicate a possible question mark over the specific items in financial statements that do not make sense (Wells 1997, p.472).

The two main types of analysis used in the detection of management fraud are percentage analysis and ratio analysis (Kranacher *et al.* 2011, p.438). It is appropriate to use more than one technique, as different types of analysis will reveal different information that may indicate possible red flags – showing that fraudulent transactions might be included in the financial statements (Golden *et al*. 2006, p.150).

Percentage analysis consists of two methods, namely: vertical analysis and horizontal analysis (Kranacher *et al.* 2011, p.438). Vertical analysis, which is sometimes referred to as common-size analysis, evaluates the relationships between items on the financial statements – by stating the different components as a percentage of a common base item (Golden *et al*. 2006, p.368). For instance, on the income statement net sales could be expressed as 100%, and all other items would then be expressed as a percentage of the net sales (Wells 1997, p.472).

The analysis is first done for a specific accounting period, and then compared with historical periods (Golden *et al*. 2006, p.368). The use of vertical analysis techniques, combined with historical averages, is very useful to determine anomalies in financial statements (Wells 1997, p.473). In larger entities, it is useful to further expand the vertical analysis too; for instance, a disaggregated basis by a business unit or in a geographical area.

This would identify outliers or specific units that drive an unusual relationship in specific items. Vertical analysis can be used to disaggregate a particular line item by the components that represent the line item, such as cost of sales that could be analysed by its underlying items, namely; materials, labour and variances (Golden *et al.* 2006, pp.368-369).

Horizontal analysis is used to understand the change of individual line items over a period of time (Golden *et al*. 2006, p.369). The percentage change is compared between accounting periods by dividing the amount of increase or decrease for each item by the base period amount. The percentages in horizontal analysis must be interpreted with vertical analysis, taking into account the monetary amount of the specific line item (Wells 1997, p.474). Through the analysis of the performance or costs on a quarterly, monthly or even weekly basis, additional trends can be identified.

For instance, if quarterly reporting is important in a specific sector, significant revenue in the last week or month before the quarter ends could be a red flag that needs further investigation (Golden *et al*. 2006, p.369).

If anomalies are identified in percentage analysis, source documentation should be investigated to determine the rise in the percentages, as this could be a red flag identifying management fraud (Wells 1997, p.474). Further investigations could include margin analysis within gross profit, or to focus on a disparity in net income as against cash balances (Golden *et al*. 2006, p.377).

Ratio analysis measures the relationship between different financial statement items and non-financial data (Golden *et al*. 2006, p.369). By evaluating the relationship and comparing amounts with industry averages, red flags can be identified (Kranacher *et al.* 2011, p.440). For instance, if there are significant changes from one year to the next, or changes over a few years, it could indicate a problem. All changes must be interpreted in the light of changes in the firm's business operations (Wells 1997, p.475).

Ratio analysis should not be considered on its own; other factors, such as the type of entity, the market conditions, and the management, should also be taken into consideration (Silverstone & Sheetz 2007, p.57).

There are various ratios that can be calculated, but generally, the nine key ratios in financial statement analysis are:

- current ratio (current assets divided by current liabilities);
- quick ratio (cash, marketable securities and accounts receivable divided by current liabilities);
- inventory turnover ratio (cost of sales divided by average inventory);
- average number of days in inventory (365 divided by inventory turnover);
- receivable turnover ratio (net sales on account divided by average net receivables);
- collection ratio (365 divided by receivable turnover),
- debt equity ratio (total liabilities divided by total equity);
- profit margin ratio (net income divided by net sales); and
- asset turnover ratio (net sales divided by average assets) (Golden *et al*. 2006, pp.371-374).

Other ratios for high-risk items, such as revenue recognition and cash or cash flow should also be considered (Golden *et al*. 2006, p.150).

Investors rely on the statements provided by investment managers to monitor their investments' performance over time. Investment managers must, on a quarterly basis, give clients a statement that enables them to produce a set of financial statements, determine the composition of the financial products, charges, as well as the market value of the investments (Millard & Hattingh 2010, p.135).

The horizontal, vertical and ratio analyses, discussed above, can be applied to individual investors' investment accounts or to the total funds under the management of the investment managers. This analysis might indicate specific red flags relating to the valuations of the clients' portfolios that need to be further investigated.

5.4.2 Reasonableness testing

Reasonableness testing is a technique used to benchmark the results in the financial statements against an independent expectation. It is particularly appropriate when the underlying account is not combined (Golden *et al*. 2006, p.369). An example, for instance, would be if the expected interest payable is calculated by multiplying the average outstanding debt balance by the average interest rate. Reasonable testing can be used with regression analysis, as it will give a reasonable forecast based on genuine inputs, to establish the prediction on which to make a comparison.

An example would be if sales are forecast based on budgets or commission expenses and the forecast is then compared with the actual sales. Variations might be a red flag that sales are overstated or understated (Golden *et al*. 2006, p.370).

Benchmarking is used by various role players in the investment management industry. It can be described as a quantifiable standard against which performance is measured (Chrisopherson, Carino & Wayne 2009, p.3). For instance, a wide variety of equity benchmarks exists. These benchmarks can be used to compare information contained in a client's statements with how a similar type of equity portfolio has performed (Chrisopherson *et al.* 2009, p.4).

5.4.3 Data-mining analysis

Data-mining analysis uses electronic software to identify and review unusual trends, patterns and anomalies within a set of data (Golden *et al*. 2006, p.386). Data-mining includes the analysis of data into patterns or relationships that have not previously existed and are important for decision-making (Silverstone & Sheetz 2007, p.58). Data mining techniques that can be used are, for instance, scanning transaction listing or identifying duplicate source documents, such as invoices or payments (Golden *et al*. 2006, p.370). This is a good detection technique to identify extraordinarily high amounts booked through journal entries at the end of a period (Golden *et al*. 2006, p.143).

One of the major drawbacks of data-mining analysis is that identifying the data can be a difficult task if there are normally various data bases from which to draw information (Albrecht *et al.* 2009, p.168).

Investment managers should have the electronic data available of all trading on clients' accounts. The regulator can use this information and apply the data-mining techniques described above, to identify any trends which might indicate unusual trading patterns that need to be further investigated.

5.5 THE USE OF INTERVIEWS TO DETECT FRAUD

Interviewing is an information gathering exercise in which people are questioned who have knowledge of specific events, people or details relating to fraud (Kranacher *et al.* 2011, p.234).

An interview with management, the audit committee, the internal auditors and other people within the organisation who might have relevant information can assist in information gathering. Focusing on specific aspects relating to areas where fraud risk might be present and obtaining collaborating evidence to certain questions could identify fraud risks and how internal controls address these risks (Golden *et al*. 2006, p.141; IFAC 2010, p.193).

It is important that interviews are organised and follows a logical path (Leinicke *et al.* 2005, p.2). Before commencing with interviews documentary evidence and records should be examined (Kranacher *et al.* 2011, p.235). This will ensure that the interview can follow a predetermined structure and result in "*meaningful fact-finding*" (Leinicke *et al.* 2005, p.2).

It is imperative to document interviews and review notes to establish if there are any themes and patterns (Leinicke *et al.* 2005, p.4). Although note taking is useful, it is not advisable to take detailed notes, listening and observing the interviewee's body language could aid in identifying any discomfort or deceit that would indicate possible red flags (Kranacher *et al.* 2011, p.237).

5.6 OTHER METHODS USED TO DETECT MANAGEMENT FRAUD

Various sources can be used to gain information relating to a company's strategy and way of doing business, as reflected in its financial statements. A good source of information is normally the media reports, industry journals or reports of financial analysts that can indicate the existence of concerns about matters directly or indirectly related to a company's financial statements. Searching public records and other internet-based databases can assist in obtaining valuable information relating to the company, its management and employees, and related parties, such as customers and suppliers (Golden *et al*. 2006, p.143).

If fictitious revenues are suspected, confirmation could well be obtained from customers – to ensure that correct contract terms are stated, and that there are no side agreements (IFAC 2010, p.193). Independent enquiries can be made to sales near the end of the period, and any unusual terms might be negotiated as they relate to these issues (IFAC 2010, p.194).

Singleton *et al*. (2006, p.130) list several other general methods, such as gauging whether the internal audit function actively engaged in proactive antifraud activities, the extent to which the external financial auditors apply fraud auditing techniques, the use of an anonymous complaints system to which employees, suppliers and customers have access and the external auditors running checks on management.

The techniques described above can also be used in the detection of investment fraud, where the focus would be on the specific performance of the investment accounts, managed by the investment manager.

5.7 RED FLAGS IN MANAGEMENT FRAUD

Red flags relating to management fraud can include accounting inconsistencies, unexpected or unusual financial performance, internal control weaknesses and aggressiveness in the executive management (Singleton *et al*. 2006, p.129). Singleton *et al*. (2006, p.129) regard the most significant of the above factors as the style of key executive managers.

If senior management have detectably low ethical behaviour, and exhibit a noticeably aggressive nature, being secretive or keeping certain information secret, this is a sign of a possible red flag (Singleton *et al*. 2006, p.129).

The fraud triangle helps to explain fraud (Singleton *et al*. 2006, p.127). The fraud triangle (as explained in **paragraph 4.3** in **Chapter 4)** provides valuable insight into the drivers that are present when people commit fraud (Singleton *et al*. 2006, pp.8-9). The three risk factors identified in the fraud triangle are: incentive or pressure (need), opportunity and rationalisation or attitude. By utilising the risk factors in the fraud triangle, red flags can be identified within an entity (Golden *et al*. 2006, p.132).

Rezaee and Riley (2010, p.107) suggest that the fraud auditor should consider, when identifying red flags relating to management fraud, the characteristics of the organisational structure and culture, board and audit committee, internal and external auditors, management, economic industry and environment, regulators, revenue and earnings, transactions and balance sheets, as well as the financial performance and business conditions.

Details on red flags applicable to management fraud that can also be used in the identification of investment fraud schemes are provided below.

5.7.1 Aggressiveness of executive management and limitations in corporate governance structures

Aggressive management styles are an indicator that the company may promote fraudulent behaviour. This indicates that the rationalisation leg of the fraud triangle is present. Where management enters into certain transactions, purely for the purpose of meeting performance objectives; and they are aggressive in setting accounting policies and are not being consistent with prior periods, and promotion is rewarded – no matter what the means were of getting there; and risk-taking is rewarded, this could indicate rationalisation on the part of management to commit management fraud (Golden *et al*. 2006, p.136).

When the "tone on the top" is inappropriate, there is a no corporate code of conduct, and the corporate mission is to maximise the profits, this indicates organisational structure red flags (Rezaee & Riley 2010, p.107). Significantly, any litigation in which the company is involved might be a sign of aggressive management who will go after anyone – no matter what (Coenen 2008, p.66).

Overly complex organisational structures, frequent changes in the structure, as well as decentralisation models with inadequate oversight – these issues can all introduce fraud risk factors that need to be considered (Rezaee & Riley 2010, p.107).

As corporate governance functions, such as the Board and its committees, especially the audit committee play an important role in the oversight of management, certain red flags – when there is a breakdown or inadequate governance – can be identified. For instance, a lack in independent directors, an inefficient board that lacks vigilance in its oversight, too much trust on executive management, and no proper risk management framework can lead to executive management overwriting of the controls (Rezaee & Riley 2010, p.107).

When considering management characteristics, several red flags can be identified. These red flags include for instance: an autocratic management; domination of the company by one or two aggressive individuals who may be egotistical; frequent turnover in management and other key staff; ineffective leadership; inexperienced and aggressive persons in key positions; the company holding a material portion of management's wealth – for instance in share options; the use of several legal councils; an aggressive attitude

towards financial reporting; executives exhibiting strong greed or being regarded as "wheeler-dealers"; management that does not see financial fraud as a risk and ignores irregularities; and management disrespect for regulatory bodies (Rezaee & Riley 2010, pp.108-109).

5.7.2 Internal control weaknesses

Management's ability to override in the internal controls can create an ideal opportunity for them to commit fraud (Golden *et al*. 2006, p.134). It is, therefore, important to be on the look-out for red flags indicating any weaknesses in the internal control environment (Coenen 2008, p.57). This would include the continuity and effectiveness of the internal audit, information technology, accounting and reporting systems and the persons working in accounting (Golden *et al*. 2006, p.134). Weaknesses in the corporate governance structure of a company with specific reference to the supervision of senior management by the audit committee and non-executive directors could indicate red flags – showing management override (Kranacher *et al.* 2011, p.175).

When management does not manage internal controls or correct deficiencies in controls or avoid disciplinary action regarding possible fraudulent activities – then, these shortcomings could indicate a possible red flag (Golden *et al*. 2006, p.136).

5.7.3 Unexpected or unusual financial performance

When a company creates unrealistic performance measures for individuals or the company as a whole, people may turn to fraud if they cannot meet these expectations (Coenen 2008, p.62).

The risk factor of incentives and pressure in the fraud triangle come into play in those cases where individual performance by aggressive incentive schemes is overemphasised, or when a company is under pressure – from external sources – to perform (Ozmen 2009, p.1).

To identify these red flags several factors must be considered. *Firstly*, an understanding of any circumstance that threatens the profitability or financial stability of the entity, expectations of third parties that might exist that would pressurise management to outperform could be relevant. These might include pressure from investors, bankers, non-compliance with listing requirements on a stock exchange, or re-evaluation of a company's position by a credit-rating agency. *Secondly*, remuneration policies and budgets could be reviewed to ascertain whether there are any threats to the personal wealth of management, due to the performance of the business or unrealistic pressure that is exerted to deliver specific performance results (Golden *et al*. 2006, p.133).

Other red flags relating to performance are when a company is outpacing its competitors in the same industry – especially when past performance was not that of the industry leader (Coenen 2008, p.63). Companies that have insufficient working capital or high levels of debt could imply higher risks for fraud, as management would find it difficult to perform with limited access to cash or restricted loan facilities (Coenen 2008, p.64).

In the case of Enron Corporation, for instance, the company was reporting outstanding revenues for several years without the cash to show for the sales. As it turned out, the revenue stream was phoney, and was created by the incorrect early recognition of revenue and the recognition of related-party transactions, as revenue when they were not (Coenen 2008, p.66).

Industry-related red flags relating to performance are, for instance, when doing business in a volatile industry or where there is a high concentration of business with a small number of customers. Rapid expansion, when not carefully planned, and deterioration in the quality of earnings over a period of time, should raise certain suspicions calling for further investigation (Coenen 2008, p.66).

5.8 TARGET FRAUD RISK ASSESMENT

Once red flags are identified, they need to be evaluated – taking into account the evidence concerning the possible existence of fraud (Rezaee & Riley 2010, p.116). Rezaee and Riley (2010, p.116) suggest obtaining supporting documentation, and then evaluating it to

determine the possibility that it may be falsified, fictitious or altered, whether it makes sense in the financial statements, in the light of the company's operations, strategic objectives, and whether there is anything else about its nature that appears suspicious.

The challenge with red flags is that there are several that can be identified, but only a handful leads to the detection of fraudulent activities (Singleton *et al.* 2006, p.131). As such, a refinement in red flag fraud detection and prevention is a target in fraud risk assessment (Rezaee & Riley 2010, p.116).

When applying the targeted risk assessment suggested by Rezaee and Riley (2010, p.116) one should focus on two areas. *Firstly*, the need to understand the type of fraud scheme that is more likely to occur – given the company, the specific industry and the operational environment that is most probable. *Secondly*, it is necessary to determine the magnitude of the possible fraud.

After the abovementioned steps have been taken, other considerations can be given to ensure closer investigation of specific fraud schemes that might be a possibility (Albrecht 2003, p.69). Some of the areas to consider are whether the fraud scheme can be rationalised, consideration of where to look for the fraud, persons who might have knowledge and who might be involved, the internal control environment that is needed to prevent the scheme, and its effectiveness (Rezaee & Riley 2010, p.116). If internal controls are adequately designed, then the likelihood of fraud is minimised (Rezaee & Riley 2010, p.21).

The owners of internal controls are the "gatekeepers", and as such, it is important to ascertain whether the owners would allow fraud "through the gate" (Vona 2008, p.29).

5.9 THE USE OF A FRAUD AUDITING APPROACH IN DETECTING INVESTMENT FRAUD SCHEMES

Steenkamp and Malan (2009, p.29) conclude that it is not easy to detect investment fraud, as there are no specific red flags that would warn investors. In a case, such as that of Fidentia, it is difficult to detect dishonesty or fraudulent behaviour that is well-disguised.

Some possible red flags would be: insufficient corporate governance, such as the chairperson and chief executive officer being the same person; no company secretary with sufficient powers; the absence of risk-management processes; financial statements that are not up-to-date; and auditors that lack independence (Steenkamp & Malan 2009, p.29).

There is limited academic literature relating to red flags in investment fraud schemes. This type of fraud, however, (as explained in **Chapter 2)** relates closely to management fraud, where investors rely on the information provided to them and ongoing performance figures to track their investments. As such, fraud auditing techniques and the red flags used in management fraud can also be used to detect fraudulent investment schemes.

In this regard, an analysis of investment returns similar to that of ratio analysis (discussed in **paragraph 5.4** above) can be applied to investment fraud schemes. Depending on the information available, specific data mining techniques on trading and performance results can be applied and compared with the industry benchmarks.

Ganshaw (2010, p.198) remarks that "*the best frauds are those that give the investors everything they could possibly hope to achieve in a legitimate investment but never more than they might rationally expect to receive*". Classical warning signs in most investment fraud cases are the marketing pitch used, and the dominance of mostly one individual in control of the scheme (Ganshaw 2010, p.191). Other red flags typically present in management fraud (as discussed in **paragraph 5.7** above) and more specifically those relating to management and governance are very relevant in the detection of investment fraud.

Investment fraud normally involves investments that have unique or complex structures that are private agreements. These are not easily understood or priced. The valuation of these investments is sometimes done by the investment manager, and this increases the likelihood for fraud (Ganshaw 2010, p.207). Fraudulent communication, in times of market distress, normally takes place, especially if the manager has declining performance and the investors have begun to redeem their investments (Ganshaw 2010, p.208).

Finding investment fraud requires out-of-the- box thinking and brainstorming (as discussed in **paragraph 5.3** above) can assist in identifying potential scenarios that fraudsters could

utilise. Lynch (2006, p.2) gives the example of an investment manager that utilised a chat room to communicate with clients and thereby avoided the companies formal communication mechanisms. This helped him to increase the price of shares in his own personal investment portfolio. To identify such scenarios the auditors had to think outside of the box and not restrict themselves at considering the formal processes and systems implemented to avoid fraud.

It is important to interview both management and employees in lower positions as they are often aware of fraud (Leinicke *et al.* 2005, p.3). In the case of Ovation (discussed in **paragraph 2.5.1**) for instance management provided false information to staff relating the pricing to investment, if the junior employees were interviewed relating pricing of investments and source of information it could have raised red flags relating the authenticity of the prices.

Doing background checks on management of investment managers as suggested in **paragraph 5.6** above will ensure that the regulator assess the "fit and proper" status of investment managers, after licensing. Any changes in the persons status should be investigated as it can be an indication of possible misconduct (Goodhart *et al.* 1998, p.6).

5.10 CONCLUSION

From the discussion above, it becomes evident that the regulator can adapt fraud auditing techniques and be on the look-out for red flags – to detect any management fraud and make it applicable to investment fraud. Even though the information relating to investment fraud is off- the-balance sheet, there must be information available relating to the clients' investments.

For some auditing techniques, such as the analytical procedures discussed (in **paragraph 5.4),** the regulator will require specific information and might need specialised tools that are not necessarily currently used. As limited information is available on the tools and techniques used by regulators, further research on this aspect might be necessary. For the other techniques discussed (in **paragraph 5.6** above), such as the searching of public records and interviews with management, these form part of the regulatory approaches

already discussed (in **Chapter 3 paragraph 3.4)**. This might require additional training for staff to ensure they can apply the techniques to identify fraud risk.

The red flags listed (in **paragraph 5.7** above) which are relevant to management fraud can also be applied to investment fraud and used by the regulator. To effectively implement a fraud auditing approach, further research on the applicability of the fraud auditing approach to different types of investment fraud has become necessary, and this needs to include consideration of red flags and the techniques needed to discover these.

CHAPTER 6:
CONCLUSIONS ON THE USE OF A FRAUD AUDITING APPROACH TO DETECT INVESTMENT FRAUD

6.1 SUMMARY OF FINDINGS AND CONCLUSION

6.1.1 Investment fraud and its similarities to management fraud

In **Chapter 2**, investment fraud was defined as the intentional misrepresentation made by investment managers, relating to investments entrusted to them by their clients (investors) that causes actual or potential prejudice to the client.

Investment fraud can originate in two ways; *firstly*, schemes that are started with fraudulent intent; and *secondly*, schemes where unrealistic expectations by the investors, or a change in market conditions can lead the investment manager to hide losses in investments from the investors – through fraudulent communication (Ganshaw 2010, p.207).

Some examples of investment fraud schemes allegedly committed by investment managers were discussed in **Chapter 2, paragraph 2.4**. These fraud cases have highlighted the issue that a lack of corporate governance and accountability by management of these entities has led to the collapse of the scheme. As can be seen from these cases, client's entrusted their funds to an external party that had the responsibility of caring for their interests. The persons in control of the companies, however, violated the trust and misappropriated the funds – and then misrepresented the facts to their clients – predominantly through false reporting that these funds were still intact; and they then used the supposed performance of these funds to attract other investors.

The investment fraud schemes were in some instances reported to the regulator. Further investigation led to the removal of management and the winding down of the schemes. The question, therefore, arises: If the regulator could have used proactive detection methods, would they have identified these investment frauds – before the facts were brought to their attention? A conclusive finding on this can only be made if the fraud

auditing approach can be simulated, based on the information available at the time of the fraud being committed. As this is not in the scope of the study, a conclusive answer can only be obtained through further research.

As described (in **Chapter 2, paragraph 2.3**), investment fraud is similar to management fraud, as it is committed by persons in positions of trust who can manipulate internal controls to falsely misrepresent the financial results of an entity (management fraud) or the off-balance sheet investments managed on behalf of clients (investment fraud).

Recent investment fraud scandals, such as that of Madoff, have prompted debate about how financial institutions should be regulated (Gadinis 2008, p.1). The IMF (2009) suggests "*a two-tiered approach to expand regulation: extending disclosure to provide enough information for supervisors to determine which institutions are big or interconnected enough to create systemic risk, and intensified functional regulation and oversight.*"

6.1.2 The regulator's role in detecting investment fraud

To achieve the suggested outcome, the regulator might have to adopt a different approach in its supervisory oversight methods, and require regulated entities to provide more detailed information about their activities – including specific information on their clients' investments. Similar to management fraud, investment fraud normally involves individuals with charming and convincing personalities. This changes the dimension of how investment fraud schemes can be detected. It requires the supervisor that searches for signs of fraud, to not only follow the money, but also consider various behavioural indicators. Consequently, it is important that regulatory staff can identify common signs (red flags) that indicate the existence of possible investment fraud.

When adopting new approaches, a regulator must be cautious that its mandate allows for such an approach. In terms of the South African perspective, the regulatory mandate, as discussed in **Chapter 3,** provides the FSB with an implied role to play in ensuring that investors are not defrauded. The FAIS Act (37/2002) has as its objective consumer protection, and as the regulator, the FSB has been assigned – in terms of the FSB Act

(96/1990) – the function of protecting consumers. Van Zyl (2004, sec.1-7) describes the ideals of consumer protection as: "*integrity, fairness, transparency and disclosure in the rendering of financial services*". This implies that the regulator should play an active role in ensuring that any entity under its supervisory sphere must uphold the law and act honestly with its clients. Although not directly stated, as in the case of the SEC and FSA, the FSB does have as its mandate to detect any fraud committed by financial institutions.

It is suggested that the FSB should consider evaluating its mandate in respect to fraud detection and to clarify mandate. One of the main reasons for regulation in financial services is to monitor (supervise) the fiduciary role in the principal-agent relationship (Goodhart *et al.* 1998, p.6).

From the discussion, in **Chapter 3**, on the different methods used by regulators, it can be surmised that the methodologies are similar. The processes differ in the different jurisdictions, but the end result – to supervise the managers and to ensure the fair treatment of clients – remains consistent. The process is based on three distinct steps. The analysis of information and documentation at the disposal of the regulator, interviews with key staff of the manager, and a scrutiny of the manager's internal controls and risk-management processes.

The SEC places more emphasis on the detection of fraud, while the FSA and FSB place their emphasis on the risk-management process.

Limited information is available on the specific methodologies used during these onsite visits. Further research on specific methodologies used by different regulators might be necessary – in order to come to a conclusive answer on whether the methodologies described can enhance the onsite techniques to such an extent, that they become cost-effective in introducing various alternative approaches.

The FSB could consider adopting the more proactive specific procedures used by the SEC to enhance its oversight of investment managers. These would include checking that the clients' investments portfolios are correctly priced, that independent reporting is done for the clients periodically, that investment management decisions are consistent with their clients' mandates, the policies and procedures for safeguarding clients' assets from theft,

loss and misuse are effective, override of controls by management, or the person in control of clients funds, does not take place, all orders placed result in best execution for the client. In addition, the accuracy of performance claims, advertisements, and other marketing materials, together with the effective disclosure of conflicts of interest can be scrutinised and tested (SEC 2010, pp.19-22).

6.1.3 The applicability of a fraud auditing approach to enhance regulatory onsite visits

Proactive fraud auditing techniques that form part of the regulator's supervisory process can assist in achieving some of the specific procedures mentioned above. Due to the overlap in control functions and the testing thereof, the FSB might also consider expanding the role of the external auditor by revising the current report, issued in terms of section 19(3) of the FAIS Act (37/2002). Here, it stipulates that the external auditor must submit this information if the manager receives client funds into a separate bank account. It must, however, be borne in mind that ISA 240 limits the types of fraud that are relevant to financial statement audits, to the misstatements resulting from any misappropriation of assets and fraudulent financial reporting (IFAC 2010, p.365), and as such, specific guidelines will have to be issued to the auditor to ensure that the intended purpose with such an audit can be achieved.

The fraud auditing approach (discussed in **Chapter 4)** is a systematic approach with different steps that require specific data to be extracted from the various financial records (real data on the operational systems) to detect possible fraud and that it focus on three main areas (Singleton *et al*. 2006, p.160). *Firstly*, the identification of the fraud scheme, since opportunities might exist that would make such a scheme likely, fraud scenarios and profiling the data need to ascertain whether the scheme exists. *Secondly*, data mining to search for transactions that meet the data profile; and *thirdly,* the fraud auditing procedures and the evidence determine whether there is possible fraud (Vona 2008, pp.28-36).

The fraud auditing approach can assist in proactively identifying fraud schemes by applying various fraud auditing techniques, such as reasonableness and completeness tests, analysing trends and statistical analysis (Singleton *et al*. 2006, p.161).

In the detection of management fraud, the fraud auditor can consider various scenarios and analyse, for instance, the performance of a company – to identify any possible fluctuations over time that could be red flags where there has been manipulation of the entity's performance. The techniques above can also be applied to detecting possible investment fraud. Investment fraud can occur, for instance, where unrealistic expectation by investors or a change in market conditions can lead the investment managers to hide losses from investors through fraudulent communication of the fund's performance (Ganshaw 2010, p.207).

Alternatively, the fraud scheme can be devised to show higher performance in investments or to be able to take higher performance fees; and as these fees are not actually earned, they would devour the client's assets over time. By applying a reasonableness and completeness test, and analysing the trends, the fraud auditor would be able to identify possible investment fraud scenarios. These, in turn, would need to be further investigated.

If compared with the processes used by the different regulators (described in **Chapter 3, paragraph 3.4),** it becomes evident that the approaches used by the different regulators in most instances are limited to utilising documentary and oral representations of management. The information gathered can be applied in a fraud auditing approach to identify fraud schemes, consider different fraud scenarios and to perform fraud auditing procedures relating to document examination and economic substance procedures.

For other procedures that are part of a fraud auditing approach, such as data mining, the regulator would need to obtain additional information.

The information can be gathered during onsite visits. Alternatively, it can be reported on a regular basis to the regulator – and through the application of certain techniques – could form part of the information to determine risk areas within the investment management industry. If the information is gathered during onsite visits, the FSB would have the power to obtain it in terms of section 4 of the FAIS Act (37/2002). Specialised computer

programmes, such as CAATS (described in **Chapter 4, paragraph 4.6.5)** would be required to extract the information and perform data mining.

If the information is to be obtained on a regular basis, the FSB would require changes to the reporting structures provided for in the FAIS Act (37/2002). Currently, the only ongoing reporting obligations are the submission of audited financial statements (section 19) and compliance reports (section 17). Further research on the type of information investment managers' report to the FSA and SEC and how this could be incorporated into the reporting obligations of the FAIS Act (37/2002), to enable proactive data mining, might be required.

To achieve the desired outcome of identifying red flags and proactively investigating possible investment fraud, supervisors would also have to be specifically trained in the utilisation of CAATs, data mining and the analysis techniques.

The other techniques (discussed in **Chapter 5, paragraphs 5.5 and 5.6**), such as the searching of public records and interviews with management, do form part of the regulatory approach (discussed in **Chapter 3, paragraph 3.4)**. To effectively use these additional techniques, it might be necessary to ensure that the regulator understands the applicability to fraud auditing.

The red flags (listed in **Chapter 5, paragraph 5.7**) relevant to management fraud can also be applied to investment fraud, and used by the regulator. To effectively implement a fraud- auditing approach, further research on the applicability of the fraud auditing approach on different types of investment fraud is necessary. This needs to include the consideration of red flags and the various techniques to uncover the different types of investment fraud.

The above discussion is concerned with whether a fraud auditing approach may be used by the regulator in the detection of investment fraud schemes. It has been found that similar techniques and red flags that are used to detect management fraud can also be applied to investment fraud. These techniques can also be used by the regulator to apply during their onsite visits, as they relate closely to current risk assessment of the overall business objectives of investment managers.

6.2 RECOMMENDATIONS

Various options in terms of the extent of implementing fraud auditing into the regulatory supervisory approach can be adopted. The regulator can consider enhancing its licensing processes by implementing proactive techniques such as the interviewing of licence applicants and the searching of public records and internet sources prior to awarding a licence. Additional consideration should be given to establish minimum criteria for corporate governance expectations and proactive monitoring of investment managers. As regulatory onsite visits apply risk assessment techniques, it could be enhanced to do specific risk assessments to identify investment fraud schemes. The adoption of a fraud auditing approach would require further research to ensure that the approach is adaptable and could be incorporated into the current supervisory approach.

A fraud auditing approach requires skilled professionals to apply a variety of techniques, depending on the specific red flags identified. In order to implement a fraud auditing approach the regulator will have to conduct a skills audit, and provide staff training to effectively utilise fraud auditing techniques.

The information required in the fraud auditing approach is recorded off balance sheet, it might be necessary for the regulator to consider specific customised software to perform data mining and analysis. There are currently no specific red flags identified for investment fraud, and as such, in the development of a sound approach to the supervision of investment managers, the regulator should consider identifying specific red flags that can be applicable to different scenarios.

The consideration of an applicable approach, when possible fraud is considered, to ensure that when a fraud audit change over to a fraud investigation, the relevant staff are not only trained in investigation techniques, but that they also understand the importance of the gathering of evidence that is admissible in criminal – as well as in enforcement proceedings.

6.3 CONTRIBUTION OF THE STUDY AND FURTHER RESEARCH

This study was limited to a literature review, and as such, interviews with investment managers and regulatory staff was not conducted. The interviewing process could provide more information relating to the methodologies used by different regulators, and by investment managers to detect fraud. Furthermore, there are limited publications in South Africa on the role of the regulator and the implementation of regulatory methodologies. The information used in the case studies, as was discussed in **Chapter 2**, to evaluate types of investment frauds in South Africa was from public documentation. Insight in additional information and other records would have made it possible to apply fraud auditing techniques.

The study has contributed in identifying alternative techniques that the regulator can apply when conducting regulatory onsite visits to investment managers to ensure that possible investment fraud is identified proactively. The limitations on supervisory resources and the high cost of resources are challenges that must be considered when introducing alternative techniques and would require additional research (Llewellyn 2006, p.7).

Fraud auditing is a relative new field for the regulator; and further research on the effectiveness of these techniques in the regulatory environment, could enhance the understanding for the regulator. Further research on the analysis of off-balance sheet information, such as investor returns and assets held on behalf of investors could well be beneficial in identifying trends.

By adapting fraud auditing approaches the regulator could become more effective in combating fraud committed by investment managers.

REFERENCES

ACFE, 2010. *Report to the nations on occupational fraud and abuse - 2010 Global Fraud Study*, USA: ACFE.

Albrecht, S., Albrecht, C.C, Albrecht, C.O & Zimbelman, M., 2009. *Fraud Examinations*. 3rd ed., USA: South-Western.

Albrecht, W., 2003. *Fraud Examination*, Ohio: Thomas Learning.

Allen, F. & Herring, R., 2001. Banking Regulation versus Securities Market Regulation. *The Wharton School of University of Pennsylvania*, pp.1-55.

Aquilar, L.A., 2009. Key note speech. In First International Conference Investment Advisors. Washington D.C. [Online] Available from: http://www.sec.gov/news/speech/2009/ spch062309laa.htm [Accessed: 2009-08-28].

Bales, K. & Fox, T.L., 2009. Evaluating a trend analysis of fraud factors. In *Academy of Accounting and Financial Studies*. Allied Academies International Conference. Las Vegas Nevada, pp. 1-85.

Baumeister, R.F. & Leary, M.R., 1997. Writing Narrative literature Reviews. *Review of General Psychology*, 1(3), pp.311-320.

Beasley, M. & Jenkins, J., 2003. A Primer for Brainstorming Fraud Risk. *Journal of Accountancy Online*, pp.1-12.

Bishop, T.J.F., Bloom, C.A., Carcello, J.V. & Cotton, D.L., 2007. Managing the business risk of fraud: a practical guide.

Black, J., 2004. The Development of Risk Based Regulation in Financial Services. [Online] Available from: http://www.lse.ac.uk/collections/law [Downloaded: 2009-09-02].

Capps, D. & Linsley, S., 2001. The Financial Services Authority's new approach to regulation. *Journal of Financial Regulation and Compliance*, 9(3), pp.245 - 252.

Carvajal, A. & Elliott, J., 2007. Strengths and Weaknesses in Securities Market Regulation: A Global Analysis. Washington: IMF.

Cendrowski, H., Martin, J.P. & Petro, L.W., 2007. *The Handbook of Fraud Deterrence*, New Jersey: John Wiley.

Chrisopherson, J., Carino, D. & Wayne, E., 2009. *Portfolio Performance Measurement and Benchmarking*, USA: McGraw-Hill.

Clauss, P., Rincalli, T. & Weisang, G., 2009. Risk Management Lessons from Madoff Fraud. [Online] Available from:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1358086 [Accessed: 2009-07-23].

Cobbett, J., 2009. Moneyweb - Special investigations - CMM entities under curatorship. *Moneyweb*. [Online] Available from: http://moneyweb.co.za/mw/view/mw/en/page91?oid= 287910&sn=Detail [Accessed: 2009-07-23].

Coburn, N.F., 2006. Corporate investigations. *Journal of Financial Crime*, 13(3), pp.348-368.

Coenen, T.L., 2008. *Essentials of Corporate Fraud*, New Jersey: John Wiley.

Comer, M.J., 2003. *Investigating Corporate Fraud*, England: Gower Publishing.

Evola, K. & O'Grady, N., 2009. As fraud schemes proliferate - are you the next investor to crash and burn? *The Journal of investment compliance*, 10(2), pp.14-17.

Fresh, A. & Baily, M.N., 2009. *What does international experience tell us about regulatory consolidation?*, The PEW Economic Policy Group. [Online] Available from: http://www.pewfr.org/project_reports_detail?id=0020 [Accessed: 2010-11-2].

FSA, 2006. The FSA's risk assessment framework. [Online] Available from: http://www.fsa.gov.uk/pubs/policy/bnr_firm-framework.pdf [Downloaded: 2010-07-02].

FSA, 2006. The FSA's Risk-Based Approach: A guide for Non-Executive Directors. [Online] Available from: http://www.fsa.gov.uk/pubs/other/arrowguide.pdf [Downloaded: 2010-10-31].

FSB, 2006. FSB Media Release: FSB places Common Cents into provisional curatorship. [Online] Available from: http://fsb.co.za/public/media/10102006.pdf [Accessed: 2009-08-29].

FSB, 2007. Curatorship of Financial Services Business of Fidentia Asset Management (Pty) Ltd and Associated Companies. [Online] Available from http://fsb.co.za/public/media/02042007.pdf [Downloaded:2010-11-02].

FSB, 2007. *Financial Services Board Annual Report 2007,* Pretoria. [Online] Available from: http://fsb.co.za/public/documents/AReport2008.pdf [Downloaded: 2009-07-23].

FSB, 2008. *Financial Services Board Annual Report 2008*, Pretoria. [Online] Available from: http://fsb.co.za/public/documents/AReport2008.pdf [Downloaded: 2009-07-23].

FSB, 2009. FSB Media release Corporate Money Managers (Pty) Ltd under curatorship. [Online] Available from: http://www.fsb.co.za [Accessed: 2010-11-02].

FSB, 2009. About FAIS Department. *Financial Services Board*. [Online] Available from:

http://www.fsb.co.za/Faisdep/about_fais_department.htm [Accessed: 2009-07-23].

FSB, 2010. *Financial Services Board Annual Report 2010*, Pretoria. [Online] Available from: http://fsb.co.za/public/documents/AReport2010.pdf [Downloaded: 2010-11-02]

Gadinis, S., 2008. Is Investor Protection the SEC's Top Priority? Evidence from Enforcement against Broker-Dealers. *American Law & Economics Association Annual Meeting*, 2008. [Online] Available from: http://law.bepress.com/cgi/viewcontent.cgi?article= 2600&context=alea [Downloaded: 2009-07-18].

Ganshaw, T., 2010. *Hedge funds humbled - The seven Mistakes that brought hedge funds to their knees and how they will raise again*, USA: McGraw-Hill.

Ghiwala, D. & Papadakis, G., 2009. *Fidentia Curators Report*, Cape Town. [Online] Available from: http://www.fsb.co.za/ [Downloaded: 2009-08-09].

Golden, T.W., Skalak, S.L. & Clayton, M.M., 2006. *A Guide to Forensic Accounting Investigations*, New Jersey: John Wiley.

Goodhart, C., Hartman, P., Llewellyn, D., Rajas-Suarez, L. & Wisbrod, S., 1998. *Financial Regulation Why, how and where?*, London: Routledge.

Gottschalk, P., 2010. Categories of financial crime. *Journal of Financial Crime*, 17(4), pp.441-458.

Griffiths, H., 2006. *Common Cents Investment Portfolio Strategists (Pty) Ltd curator's first report to Court*, Cape Town. [Online] Available from: http://www.commoncents.co.za/documents [Downloaded: 2009-08-08].

Hofstee, E., 2006. *Constructing a good dissertation. A practical guide to finishing a Master's, MBA or PhD on schedule*, Sandton: EPE.

Hutter, B.M., 2005. The Attractions of Risk-based Regulation: accounting for the emergence of risk ideas in regulation. [Online] Available from: http://citeseerx.ist.psu.edu [Downloaded: 2010-07-04].

IFAC, 2010. *International Standard on Auditing 240*, International Federation of Accountants. [Online] Available from: http://web.ifac.org/download/a012-2010-iaasb-handbook-isa-240.pdf [Downloaded: 2009-11-18].

IMF, 2009. IMF Urges rethink of how to manage global systemic risk. *IMF Survey.* [Online] Available from: http://www.imf.org/external/pubs/ft/survey/so/2009/POL030609A.htm [Downloaded: 2009-11-18].

Institute of Directors, 2009. King Report on Governance for South Africa.

IOSCO, 2010. Objectives and Principles of Securities Regulation. [Online] Available from: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD323.pdf [Downloaded: 2010-07-

04].

Ivancevich, J.M., Duening, T.N., Glibert, J.A. & Konopaske, R., 2003. Deterring White-Collar Crime. *The Academy of Management Executive*, 17(2), pp.114-127.

Iyer, N. & Samociuk, M., 2006. *Fraud and Corruption: Prevention and Detection*, England: Gower Publishing.

Jarvis, C., 2000. The Rise and Fall of the Pyramid Schemes in Albania. *International Monetary Fund Staff Papers*, 47(1), pp.1-29.

Koornhof, C. & Du Plessis, D., 2000. Red flagging as an indicator of financial statement fraud: The perspective of investors and lenders. *Meditari Accountancy Research*, 8, pp.69-93.

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

Langevoort, D.C., 2009. The SEC and the Madoff Scandal: Three Narratives in Search of a Story. *Georgetown Law Faculty working papers*.

Leinicke, L.M., Ostrosky, J.A., Rexroad, W.M., Baker, J.R. & Beckman, S., 2005. Interviewing as an Auditing Tool. *The CPA Journal*, pp.1-4.

Llewellyn, D.T., 2006. Institutional Structure of Financial Regulation and Supervision : The Basic Issues. In *World Bank Seminar*. Aligning Supervisory Structures with Country Need. Washington D.C. Available from: http://siteresources.worldbank.org/INTTOPCONF6/Resources/2057292- 1162909660809/F2FlemmingLlewellyn.pdf [Downloaded: 2010-07-04].

Longo, J.M., 2009. *Hedge fund alpha: a framework for Generating and Understanding Investment Performance*, USA: World Scientific Publishing.

Lynch, A., 2006. Think like the fraudster: brainstorming how fraudulent activities may occur can open the auditor's mind to a host of new possibilities. *Internal Auditor*, pp.1-4.

McCool, G. & Graybow, M., 2009. Madoff gets 150 years for massive investment fraud. *Reuters*, [Online] 29 June. Available from: http://www.reuters.com/article/idUSTRE55 P6O520090629 [Accessed: 2009-12-19].

McCrary, S.A., 2002. *How to create and manage a hedge: A professional's guide*, New Jersey: John Wiley.

Millard, D. & Hattingh, W., 2010. *The FAIS Act Explained*, South Africa: LexisNexis.

Mouton, J., 2001. *How to succeed in our Master's and Doctoral studies*, Pretoria: Van Schaik.

Muhtaseb, M.R. & Yang, C.C., 2008. Portraits of five hedge fund frauds. *Journal of Financial Crime*, 15(2), pp.179-213.

Nel, H.C., 1999. The Plight of Victims of Economic Crime: Investors as Victims. *Journal of Financial Crime*, 6(4), pp.311-322.

Ozmen, K., 2009. Managing The Risks Of Fraud In A Downturn. *PriceWaterhouseCoopers*. [Online] Available from: http://rbd.doingbusiness.ro/ro/3/articole-recente/6/244 [Accessed: 2011-01-20].

Pearsall, J., 1999. Concise Oxford Dictionary. In *Concise Oxford Dictionary*. New York: Oxford University Press.

Peterson, B. & Levin, J.A., 2007. *Curator's First Report - Ovation companies*, Cape Town. [Online] Available from: http://www.ovationglobal.com/visitors/default.asp [Downloaded: 2009-08-08].

Pillay, C., 2008. SADC must block financial fraud. [Online] Available from: http://www.faisombud.co.za [Accessed: 2009-07-23].

Pressman, 1998. On Financial Frauds and Their Causes -. *American Journal of Economics and Sociology - Wiley Online Library*, 57(4), pp.405-421.

Raw, C., Page, B. & Hodgson, G., 2005. *Do You Sincerely Want to Be Rich?: The Full Story of Bernard Cornfeld and I.O.S. (Library of Larceny)*, USA: Broadway Books.

Rezaee, Z., 2002. *Financial Statement Fraud Prevention and Detection*, New Jersey: John Wiley.

Rezaee, Z. & Riley, R., 2010. *Financial statement fraud prevention and detection* Second., New Jersey: John Wiley.

Robinson, P., 2007. FSA Financial Crime Conference : Closing remarks. In FSA Financial Crime Conference. United Kingdom. [Online] Available from: http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2007/0122_pr.shtml [Accessed: 2010-07-06].

Sander, P., 2009. *Madoff*, USA: Lyons Press.

SEC, 2010. Examinations by the Securities and Exchange Commission Office of Compliance Inspections and Examinations. In SEC Speaks 2010 Conference. Washington D.C.

Shain, R., 2008. *Hedge Fund Due Diligence: Professional Tools to Investigate Hedge Fund Managers*, New Jersey: John Wiley.

Silverstone, H. & Sheetz, M., 2007. *Forensic Accounting and Fraud Investigation for Non-Experts* 2nd ed., New Jersey: John Wiley.

Singleton, T. & Singleton, A., 2007. Why don't we detect more fraud? *Journal of Corporate Accounting & Finance*, 18(4), pp.7-10.

Singleton, T.W., Singleton, A.J., Bologna, G.J., Lindquist, R.J., 2006. *Fraud Auditing and Forensic Accounting* 3rd ed. New Jersey: John Wiley.

Snyman, C., 2007. *Criminal Law* Fifth Edition., South Africa: LexisNexis.

Solaiman, S., 2009. Investor protection by securities regulators in the primary share markets in Australia and Bangladesh - a comparison and contrast. *Journal of Financial Crime*, 16(4), pp.305 - 333.

South Africa. 2002. Financial Advisory and Intermediary Services Act, No. 37 of 2002. *Government Gazette*, 449(24079):1-37. [Online] Available from: http://www.info.gov.za/view/DownloadFileAction?id=68072 [Downloaded: 2011-01-15].

South Africa, 2001. Financial Institutions (Protection of Funds) Act, No. 28 of 2001. *Government Gazette,* 437(22857):1-16. [Online] Available from: http://www.fsb.co.za/ [Downloaded: 2010-11-02].

South Africa, 1990. Financial Services Board Act, No. 96 of 1990*. Government Gazette,* 447(21141):1-16 [Online] Available from: http://www.fsb.co.za/ [Downloaded: 2010-11-02].

South Africa, 2004. Securities Services Act, No. 36 of 2004. *Government Gazette,* 475(27190):1-124, [Online] Available from: http://search.sabinet.co.za/netlawpdf/netlaw/Securities% 20Services%20Act%2036%20 of%202004.htm [Downloaded: 2010-11-02].

Steenkamp, P., 2007. *Fidentia: A Strategic and Corporate Governance Analysis*. Stellenbosch: University of Stellenbosch. [Online] Available from : http://scholar.sun.ac.za/bitstream/ handle/10019.1/802/Steenkamp_Fidentia_2007.pdf?sequence=1 [Downloaded: 2010-11-20].

Steenkamp, P. & Malan, D., 2009. How safe is safe? *USB Leaders' LAB*, pp.26-29.

Stewart, S., 2005. Coping with the FSA's risk-based approach. *Journal of Financial Regulation and Compliance*, 13(1), pp.43-47.

Stulz, R.M., 2007. Hedge Funds: Past, Present, and Future. *Journal of Economic Perspectives*, 21(2), pp.175-194.

Tickner, P., 2010. *How to be a successful frauditor*, New Jersey: John Wiley.

Tieman, F. & Cihák, M., 2008. *Quality of Financial Sector Regulation and Supervision Around the World*, International Monetary Fund Working Papers, pp 1-45 [Online] Available from: http://ssrn.com/abstract=1266523 [Downloaded: 2010-11-02].

Van Zyl, F., 2004. *Financial Advisory and Intermediary Services Manual*, Cape Town: Juta.

van de Bunt, H., 2010. Walls of secrecy and silence. *Criminology and Public Policy*, 9(3),

pp.435 - 453.

Vona, L.W. 2008. *Fraud Risk Assessment*, New Jersey: John Wiley.

Wells, J.T. 1997. *Occupational Fraud and Abuse*, Austin, Texas: Obsidian Publishing Company.

Wells, J.T. 2008. *Principles of Fraud Examination* 2nd ed., New Jersey: John Wiley.

World Bank & IMF, 2005. *Financial Sector Assessment: A Handbook*, Washington D.C.