GÖTEBORGS UNIVERSITET

ROLES OF FINANCIAL EXPERTS AND INFORMATION TECHNOLOGY IN FINANCIAL FRAUD DETERRENCE

A THESIS SUBMITTED TO

THE FACULTY OF INTERNATIONAL ACCOUNTING PROGRAM

IN CANDIDACY FOR THE DEGREE OF

MASTERS IN INTERNATIONAL ACCOUNTING

DEPARTMENT OF GRADUATE SCHOOL OF BUSINESS

BY

MS. RUCHI DUBE

GOTHENBURG, SWEDEN

This essay is dedicated to my parents, Mr. Nandan Dubey and Mrs. Usha Dubey, my sister Ms. Archita Dubey,
- and my brother Mr. Vatsal Dubey -

There is no little enemy. Opportunity makes a thief. A door must either shut or open. The squeaky wheel gets the grease. Diligence is the mother of good luck. A cat in gloves catches no mice. Diamond cuts diamond.

[A Collection of Book's Chapter Epigraphs]

—Pickett, K.H. & Pickett, J. (2002) Financial Crime Investigation and Control. New York.
John Wiley and Sons, Inc

Table of Contents

ILLustrations

Tables

Preface

The origin of the research was through a brief period of study on International Accounting Standards, which stressed that unified accounting principles improved transferability in global settings and guaranteed more transparency. Frauds in multinational companies formed an integral part of the literature, which is as an eminent cause of massive losses in businesses. The theory for this thesis is evaluating which financial processes have common cases of fraud. The internet documents from Google search results varied with many writing about recent fraud charges against corporations. The past scandals provided brief insights into types of corporate fraud. It generated a deep research on industry frauds and all types of weaker business areas. The search depended on popular media headlines from the business world. Therefore, mergers and acquisitions, and risk management were topics of great interest. Needless to state, but financial fraud had many categories that engulfed these research documents and caught attention because of the problem's vividness. The documents evaluated the impact of each fraud. After viewing the expanse on the subject, it became relevant that each basic fraud in financial statements or business transactions needed attention for closer summary. Some of the major search terms on business processes targeted the extent of fraud instances and involvement of employees. The topic of the research was to find global-level processes that were susceptible to fraud in the multinational companies. The major time of document review on this matter occurred between September 2005 and March 2006. It was a definitive introduction to the fraud detection and correction. During the meeting, the adviser suggested that thesis will become too broad form different frauds point-of-view, and from here professions may become a matter of study, and antifraud tools or steps used by employees may become research subjects based on literature review of fraud and correction-centered roles of the auditor, board of directors, management, and forensic accountant.

During summer of 2006, a major involvement for the thesis was from a hypothetical Swedish-Swiss NYSE-listed company X, at which the corporate intranet documents on internal control were collected from a sample of adequate data that ranged from several categories of business. The range of intranet documents turned disjoint at times from one another, and was identical with process-based review on business frauds. It provided an added opportunity to analyze the roles and responsibilities of professionals versus organizational interests in business processes that used special in-house company software tools. Corporate governance from here became theoretical analysis subject for the thesis. Between mid-September and November 2006, a close review of literature books revealed vast amount of data related to roles of corporate governance members, forensic accountant, and other professionals that may become resourceful in fraud-prone business processes. These business processes needed tally from internal control processes of company X to find some of the susceptible areas during everyday functioning of financial business transactions. It made understanding software and information technology a solution to studying about fraud. After reading the thesis, major corporate stakeholders can receive an answer about which professional uses what theoretical finance or accounting antifraud theory, and how does the professional deliver the idea through internal control reporting software tools, besides compliance, financial reporting, planning and budgeting, surveying, and collaboration issues.

Acknowledgements

I will chiefly express the contributors from Handelshögskolan, Göteborgs Universitet. My deep regards to Professor Ulla Törnqvist, who guided me throughout the thesis patiently as an adviser. In several instances and many Masters courses, Professor Thomas Polesie provided intellectual upheaval to me as his student. I also express my gratitude to Ms. Ann McKinnon who supported my stay as a foreign student in Sweden throughout the program.

It is also important to recall empirical contributors. This study could have become a failure without support from Mr. Nandan Mahimkar and Mrs. Ann-Therese Kirkland. I thank Mr. Johan Andersson, Ms. Lillian Furusjö and Mrs. Kelley Nilsson-Petersson who advised me about the thesis.

Abbreviations

A&RG - Accounting and Reporting Guidelines (US GAAP)
ACFE - Association of Certified Fraud Examiners
AICPA - American Institute of Certified Public Accountants
AP – Accounts Payable
AR - Accounts Receivable
ASB - Auditing Standards Board
BI – Business Intelligence
BPM - Business Performance Management
BRC - Blue Ribbon Committee
CAATs - Computer assisted audit techniques
CCM - Continuous Controls Monitoring
CEO - Chief Executive Officer
CFO - Chief Financial Officer
CIO - Chief Information Officer
COBIT - Control objectives for information and related technology
COSO - Treadway Commission of Sponsoring Organizations
CPA – Certified Public Accountants
ERP – Enterprise Resource Planning
EU - European Union
FX - Foreign Exchange
GAAP - Generally Accepted Accounting Principles
GAAS - Generally Accepted Auditing Standards
GAS - Generalized Audit Software
GL Accounts – General Ledger Accounts
IBM - International Business Machines
IIA - Institute of Internal Auditors
IR - Interest Rates
IS - Information Systems
ISACA - Information Systems Audit and Control Association
ISO - International Standards Organization
IT - Information Technology
NYSE - New York Stock Exchange
PCAOB - Public Company Accounting Oversight Board (U.S.)
PDF - Portable Document Format
PoS – Point of Sale
SAS - Statement of Auditing Standards
SEC - U.S. Securities and Exchange Commission
SEPA - Single European Payments Area
SoD – Segregation of Duties
SOX / SOA - Sarbanes Oxley Act 2002
SWIFT - Society for Worldwide Interbank Financial Telecommunication
TSE - Toronto Stock Exchange
XBRL – eXtensible Business Reporting Language

Glossary

1. Audit Trails - A history of activities by transaction, posted because of operations on specific data. Operations are events (by transparent event descriptors) noted in the audit trail because of a particular session with the database.
2. Auditor Walkthroughs - Internal and External auditors view, capture, and publish evidence related to an audit session that insures proper internal controls functioning.
3. Dashboards - Customized computer screens that show key performance indicators that aid managers to react to changing business conditions.
4. Forensic Accounting Professions - "Forensic Accountants" are members of a broad group of professionals that includes those who perform financial investigation, but it is wider. The public often uses the term "forensic accountants" to refer to financial investigators, although many forensic accountants do not perform financial investigations. Forensic accounting investigators train in investigating and resolving suspicions or allegations of fraud through document analysis to include both financial and nonfinancial information, interviewing, and third party inquiries, including commercial databases. It is important to recognize the responsibility of the company to conduct a thorough investigation in any matter that can be material to the financial statements. Whatever authority the forensic accountant has in the conduct of the investigation, it is not the forensic accountant's investigation; it is the company's initiative. This does not release forensic accountants from the ethical duties and rules needed by their professional associations, like the ‘American Institute of Certified Public Accountants’ (AICPA) and the ‘Association of Certified Fraud Examiners’ (ACFE).
5. Queue - A queue is an “inbox” for work of a specific classification. Users are able to view all queues in the computer network and drill down into the individual queue to look at the total number of work objects, and the number of incoming and outgoing work objects over a named time period.
6. Red Flags - Early Symptoms of frauds used by internal and external auditors
7. SAS 70 Type II - Auditing standard that guides on physical security of documentation.
8. Workflow - Automation of documentation flow in particular folders with periodic routing or as assigned in an enterprise.

ROLES OF FINANCIAL EXPERTS AND INFORMATION TECHNOLOGY IN FINANCIAL FRAUD DETERRENCE

BY

MS. RUCHI DUBE

AND SUPERVISED BY

PROFESSOR ULLA TÖRNQVIST

Abstract

Governing bodies pass rules to provide accurate financial reports to investors. Increasing cross-border mergers and financial services have lead to demand for international professional standards that deter fraud risks in auditing, accounting, and other financial services. Most financial organizations have specific roles for their corporate governance members, or employ specialized services of forensic accounting investigators, technologists, and forensic accountants to detect fraudulent financial activities. These financial professionals target industry-specific fraudulent schemes and apply correctional tactics by using computer software that include document management, data mining, business performance management, and compliance tools. The present study examines kinds of software used by forensic service professionals and corporate governance members to deter financial fraud. The results indicate that information technology provides professionals with extensive scope to deter financial fraud in transaction-level controls.

Chapter One

❖ *Introduction to the Study*

Most multinational companies depend on the power of financial controls to certify the sanctity of performance measures. In fact, accountancy and finance portray numbers and theory to describe a business, where numbers foretell degree of efficiency. There are steep differences in mere theoretical and numerical explanations, which stimulate strong urges to manipulate the final opinion in a particular direction. A downfall in media ratings and stock-prices is a common sign of finance and accountancy pitfalls that can hint a particular fraud. Major legal cases, like Enron and WorldCom, have represented the study of frauds.

Some areas in Finance form studies on management, occupational roles, and measurement of financial reporting risks. The purpose of studying financial risks is to prepare for unplanned losses that may lead to massive disruption of business. From here, risk control for financial frauds can comprise of study on a particular field of financial frauds, and on professionals who must strive to control any misappropriations. In fact, the subject of occupational risks pays special attention to the roles of individuals and their skills that are a precondition before facing problems at work. Thus, particular professionals that are more susceptible to known frauds must use internal control measures for countering financial reporting risks.

Global stock market financial analysts conduct checks on “practice known broadly as ‘accounting manipulation’ which encompasses earnings management, including income smoothing and ‘big bath’ accounting, and creative accounting. Although listed firms gain by constant scrutiny of financial markets and have to match the efficiency of market analysts that estimate risks through cash flow and ratios, calculated manipulation to allow a wanted accounting treatment for changing investors' opinion of the risk leads to frauds when the result is outside the limits of accounting laws and standards" (Lebas and Stolowy 2002). Therefore, professionals need to guard against aggressive accounting in financial statements of their corporation to foster investor confidence.

To settle, corporate governance members and forensic service specialists that take part in insuring accurate financial reporting must display efficiency in countering financial frauds, by detecting and resolving through software, and interacting with other kinds of occupations on its discovery. Therefore, further research must assess the efficiency experienced by financial experts when they use 'information technology' (IT) software to detect fraud, or stop its likelihood through improved internal control reporting and risk assessment.

1) Background of the Study

Since the act of the Sarbanes Oxley (SOX/SOA), compliance for internal controls is in effect, at most multinational corporations listed on the New York Stock Exchange (NYSE). The act has two major sections- 302 and 404 that targeted major multinational corporations. It has lead to a sharp increase in compliance and internal control reporting software use. Another important global standard setter is the European Union (EU) that fosters international unity of financial markets. The EU plans to set up universal banking for securities trading throughout member countries by ensuring uniform practice of 'Single European Payments Area' (SEPA) rules for payment. It has already carried out European single currency- Euro. It means that financial institutions as banks or stock exchanges can use 'International Standards Organization' (ISO) coded 'Society for Worldwide Interbank Financial Telecommunication' (SWIFT) messaging for rapid electronic transfers. These advances are visible examples of internationalized IT efficiencies in tracking data through planned templates that stand for particular types of transaction in electronic transaction between various interested parties like banks, brokers, stock exchanges, and more.

Most businesses that employ software for compliance, internal control, human capital management or others, benefit from detecting fraudulent reports and documents on routine. Many corporations offer IT solutions that try to deter fraud. The rise of forensic accounting professions that are fraud-experts is the newest development, which is not always a common role in most countries of the world.

2) Problem Statements

The general question this study will try to answer is this one: "*How can various IT-solutions help different professionals about detection and correction of financial frauds?*" That general question covers several related questions:

> *What are the roles of Corporate Governance members and forensic services specialists in the deterrence of financial fraud?*

The theory includes a fraud deterrence outline, like active oversight by the Board of Directors, Audit Committee, code confirmation, management's involvement in financial reporting and override of controls, organizational procedure to receive, hold and treat complaints of fraud, internal and external audit effectiveness, fraud risk assessment and adequacy of internal controls (Stone 2005).

> *What are some of the areas in a functioning business entity where internal control may insure compliance with section 404 of Sarbanes Oxley act?*

The rational depiction of designed internal controls in business must answer critical control objectives and the roles segregation between different actors in the organization. Varied contents of business reporting templates will further elaborate a comparative study between different types of software, based on internal controls of a business entity. Internal control assessment that states control objectives and procedures is the heart of fraud deterrence.

> *How do the following kinds of software and related others assure effective internal control reporting of the business?*
>
> - *Generic software tools for Accounting, Communication and collaboration, and Regulatory and technical reference*
> - *Document Management and Workflow Software Tools*

- *Data mining, file retrieval and pattern recognition*
- *Business Intelligence*
- *Business performance management*
- *Real-time compliance tools (Winters 2004)*

Control design and execution are as important as setting control objectives. To analyze the difference between the control objectives, that is what to perform versus control procedures (what is complete), it is essential to evaluate the different uses of IT. A review of different kinds of software that can focus on the business environment, employees, policies, and procedures will provide insight on software tools that identify weaknesses in internal controls and recommend more computer solutions that can impose accuracy in financial reporting. The research must insure the reader understands methods that assure deterrence or discouragement of unauthorized consumption or exploitation of the company assets through identifying internal and external causes.

Which technology helps the members of corporate governance and forensic specialists the most?

Most early researches on IT tools and frauds yield listing of software companies that offer solutions for credit card and check frauds. Therefore, the thesis tries to understand the areas where software can possibly resolve complications that arise because of fraudulent reporting. The thesis must understand current terminologies in technology that can aid in overseeing risks to financial stability. After conducting the research, the conclusion must depict the professional roles in IT environment. The thesis must include an outline of which internal control reporting software resolves most threats of fraud, and offer the best deterrence services, as judged by the researcher. It must suggest the most advanced software in surveying business that participates in detection and prevention of frauds. The answer will broadly depict the current stature of antifraud software.

3) Purpose of the Study

The study contributes to the growing literature on fraud deterrence and benefits of installing effective IT solutions. It studies theory of corporate governance and the professional roles of individuals who engage intensively in fraud deterrence. The purpose of the study is as follows:

> *To understand internal controls and identify where the organization battles frauds in computers based environment, with extensive scope towards understanding software and professional roles that can insure fraud deterrence.*

The research aims to study technology enabled business practices. It develops a foundation of necessary skills to manage specific business procedures, especially in the knowledge of software within an enterprise. It can inspire for education in specific kinds of software used for internal controls and study developments in technology like real-time financial reporting.

4) Professional Significance of the Study

There are many benefits in knowing more about information technology. Many large corporations use 'Enterprise Resource Planning' tools (ERP) to resolve financial problems. The study must involve studying one of the major ERPs, and using the resulting information for advancement in the computer knowledge. It responds the need to learn financial software and understand internal control for efficient cooperation during problems of fraud with the members of corporate governance.

5) Thesis Outline

The thesis has six chapters, with chapter two on research method, chapter three describing the theory, chapter four explaining the results, chapter five on the analysis of empirical results, and finally chapter six that ends the thesis. The next chapter will describe the subjects of the study, and the contexts of gathering data to analyze frauds, IT, and professional roles.

Chapter Two

❖ *Thesis Methodology*

Every thesis has a basic plan for gathering empirical evidence. Some early choices must decide on the empirical that suit the study the most. This chapter will explain the choices and the reasons to use a particular method.

1) Research Perspective

The research applied qualitative approach, which focused on gathering and grouping data on internal control composition, kinds of software that deter fraud, and transaction-level controls. The research used the constant comparison method for grouping and coding. Qualitative research compels that methods and theories be suitable for a particular study; new outlook emerge from existing theories. The qualitative study can never depend on measurements in quantities, but depends on the reality in an organization. It allows for different viewpoints of the researchers and the collected data.

Research Approach

The research approach was through constant comparison study. The approach strived to review information from written documentation on internal control arrangements that try to erase financial reporting risks and kinds of software for internal control reporting. It is important to assess risks in concrete business environment. Therefore, a study on internal control layouts can provide examples to judge the adequacy of software used in internal control reporting. Further, IT tools that offer antifraud services must also represent assimilated internal control features, which need review of technical specifications.

The main decision for the chosen approach is to depend on software as a tool to carry out transaction-level controls, as these controls depend strongly on the organization's internal control policies that always aim to prevent fraud. Therefore, guidance on efficient display of chosen secondary data is apt in the fields of internal control practices and software.

Any research will not suffer from narrow-mindedness, if documentation is reliable, and from a large organization, that needs internal controls in effect. It could provide better results than interview comments, when condensing the documents is proper and use of the documents is for major practical purposes in an organization. The research originally used published data from a corporation, which resolved no need for rapid generalization of opinions of chosen people in interviews and surveys. Therefore, the characteristics of the qualitative data depended on valid document observation with the constant comparison method for the loci of topics. Thus, the study aimed to identify where organization faced fraud risks in computers-based environment, besides understanding professional duties.

2) Context of the Study

The specialty of the research was that it tried to document real internal control procedures from an assumed Swedish-Swiss company X, which must ensure compliance to SOX section 404, because of its listing on the NYSE. The company X data comprised of information, which was available on the company's intranet between June 22 and September 15, 2006. One of the corporate offices in Sweden granted exclusive access to the intranet data, which provided time and focus only on this company and not on several others through research methods like surveys or interviews, because it was unnecessary to reach out for more data. The company's intranet had information on SOX 404 project with process-specific guidelines. The researcher used project documents after sampling internal control-related data. However, more information was available on the intranet in internal control method files that recounted employee duties and document handling for internal circulation at company X. The internal control MS-Excel files contained samples of usable information on Accounting related objectives, but the thesis does not mention data on employee duties to maintain integrity of the company. Observations revealed that error in handling data, timing and some other financial reporting risks were repetitive of the following:

- Data entry without acceptable authorization
- Wrong data entry and/or in the wrong accounting period
- Inadequate Segregation of Duties (SoD)
- Duplicate or nonexistent data posting of material items like invoices or purchase-orders
- Not performing actions of significant monetary worth related to an internal control and/or with wrong timing for posting that data
- Estimates of items like inventories are wrong

Therefore, mention of redundancies related to repetitive nature of risks was only for some internal control practices, and reference notes tried to explain missing information for the others. Some of the internal control descriptions also had information related to dependency on SAP technology. This information displayed basic underlined examples from company X with more IT roles that could employ other types of software for effective antifraud controls. The idea was to inter-link technology use in company X with other kinds of internal control reporting software that can ease in creation and management of internal controls. In judging redundancies, the files viewed first mentioned most of the data, and the files that sounded repetitive of risks or unimportant internal control methods during later observations had no summarization. The results section included reference as footnotes for clarification of sampled information for reading ease.

The choice of software firms appeared after narrowing the list of sellers for different software that aid in internal control reporting from an article on the internet by Mr. Bruce Winters (2004). A sample of sellers from this article broadly described the following software types:

- Business Intelligence
- Compliance
- Data Management
- Fraud Detection
- Business Performance Management

- Process Management
- Transaction Systems

Each seller offered tools for key tasks and for each software. For simplification, grouping of all key features from different sellers described the software's scope in internal control reporting.

The thesis relied first on company X internal control methods and second on software description to give a link between technology and financial controls, which could simplify in reducing frauds risks. The context of this study depended on analysis of documents from company X, internet and literature books to summarize internal control issues, types of frauds, features suited to transaction-level controls, and special software.

3) Research Design

This research used only secondary data; considering the data had a different purpose originally. The secondary data implied using document observation and applying at least one basic comparative method. As stated before, the constant comparison method was the method of choice, as described from now:

The Constant Comparison Method

This method runs on a set of field notes. The basic composition of this method includes coding, grouping, writing field memos, and finally forming a hypothesis. The constant comparison method used theoretical definition of transaction-level controls, and types of frauds for background. Besides this, the internal control templates from company X and tools of software firms drew up other areas to setup this method for producing thesis results. The table below depicts the style for using the stated method:

Table 1: Constant Comparison Method

Qualitative Method Questions
Is the software solution a part of the Fraud Deterrence Cycle?
What are different classifications of transaction-level controls?
What involves software with fraud deterrence?
What are the different kinds of software firms involved?

Coding and Grouping: A particular internal control reporting software ~~type~~kind includes grouping of software features by every software firm in a combination. Therefore, same vendor can have codes more than once in separate software. Similarly, grouping and combining of all available control templates from company X can result in one reference for all reporting methods. Then, a single code could represent that reference for whole subset of control templates for company X, but individual internal control procedures could still hold grouped data expressed in separate tables.

Field Notes: The data from company X held necessary amount of notes on different internal controls, and mention of financial reporting risks was rarer to reduce the sample size for results. Notes also originated from theory on transaction-level controls and frauds. Winters (2004) adequately summarized most notes for business software in his articles, which might be suitable for introduction to different software.

Hypothesis: The transaction systems and ERP are most popular software for managing frauds. ~~Such~~These software exists as stand-alone solutions, but offers various tools for recording inaccurate transactions. Most frauds occur at the point where exchange of funds takes place, and so curbing frauds is best possible by transaction systems and ERPs like SAP, since the software promotes accurate monetary transactions. To test this hypothesis, the results section will use the coding, grouping and field notes mentioned above and recount the benefits of transaction systems and ERPs against other internal control reporting software that helps in deterring financial frauds in any business.

4) Collection of Data

Collecting software data assumed feasibility of grouping it later under set categories for internal control reporting tools. The idea was to study some of the major categories of software, but not general collaboration or basic accounting tools, leaving aside SAP *(Coded as [ERP])*, because company X used this software for ensuring internal controls for financial transactions in Sweden. For control processes, grouping of data as a single unit was for comparison within notes for each process later. *Most fraud types needed a sign (Coded as [F]). In addition, all the following company X Processes belonged to one category that represented internal control processes (Coded as [A]):*

- *Accounts Payable*
- *Accruals and Provisions*
- *Cash Funds*

- *Commitments & Contingencies*
- *Financial Reporting*
- *Financial Management*
- *Intangibles*
- *Inventories*
- *Information Technology*
- *Payroll*
- *Property, Plant & Equipment*
- *Projects*
- *Purchasing*
- *Revenues and Accounts Receivables*
- *Shareholders Equity*

Intercomparison in the processes with another is possible, however the processes offer a collection of control objectives for efficient financial reporting, and recurring risks that hamper financial reporting. The processes also combined transaction-level controls as defined by the 'Treadway Commission of Sponsoring Organizations' (COSO) agenda for fraud deterrence. The internal control data provides basis for benefits drawn after implementation of particular software, based on practices performed at company X, which speak of document circulation, process-flow, workflows, and transactions, if not planning and budgeting by managers. Thus, the internal control processes can influence software use.

Further, the major grouping of software that represents most features of transaction-level controls follows in the table below:

Table 2: Software codes for comparison

Kind of Software ~~Type~~	Vendor Grouping	Codes
Business Intelligence	Hyperion, BusinessObjects, Cognos	BI
Compliance	Certus, Paisley, Axentis Enterprise (Ae), BusinessObjects, Handysoft BizFlow, IBM, Movaris	C
Data Management	FileNet, eFileCabinet, GoFileRoom, EMC, Hyperion, ACL, IBM	DM
Fraud Detection	IDEA, ACL, BusinessObjects, IBM, Axentis Enterprise	FD
Performance	Cognos, Extensity, BusinessObjects	PM
Process	Handysoft BizFlow, Metastorm	P
Transaction Systems	IDEA, ACL, Approva, Movaris, Extensity	TS

5) Delimitations

The limits of the research were its broad dependencies on different and linkable theory sets. In a major way, the data collected was secondary in nature with large amount of scope to resolve thesis problem statements. The kaleidoscope of the data needed to rely on some form of cross-comparison and accurate implementation to reduce confusion. Although, uses of company-originated genuine documents are favorable, the data was secondary in nature. Another issue was timing the research.

6) Data Analysis

The data analysis takes place in the following chapters where the results section will use coding, grouping, and memo model of the constant comparison method. The empirical results will use the codes for testing the basic hypothesis for the constant comparison initiative, which will succeed by the results analysis and conclusion. Further data analysis will continue until the closing chapter of this thesis, with next chapter describing Fraud Deterrence Cycle, transaction-level controls, corporate governance, and related professionals.

Chapter Three

❖ *The Theoretical Framework*

The aim of this chapter is to provide an insight into the roles of different financial experts or professionals. The chapter is subdivided into three major parts that describe fraud, corporate governance, and forensic financial services. It also provides answer to questions on corporate governance and forensic accounting roles in deterring frauds.

1) Financial Fraud – Simply Stated

Fraud is briefly defined as “any crime for gain that uses deception as its principal modus operandi. There are four legal elements that must be present: (1) a material false statement, (2) knowledge that the statement was false when it was uttered, (3) reliance on the false statement by the victim, and (4) damages as a result” (Wells 2005).

Fraud versus Error - Errors are unintentional misstatements or omissions of amounts or disclosures in financial statements. Errors involve mistakes in gathering or processing financial statement raw data, unreasonable accounting estimates, or mistakes in application of accounting principles related to amount, classification, manner of presentation, or disclosures.

a) Fraud Deterrence Cycle

Skalak et al (2004) stated “the extent of fraud deterrence cycle involves four elements: (1) corporate governance, (2) transaction-level controls, (3) retrospective examination, and (4) investigation and remediation. Below is a shorter description of the components:

i) Corporate Governance

The nature of corporate governance as an entire culture that sets and monitors behavioral expectations intended to deter the fraudster. Some of the key reform issues include meeting increased demands and expectations of investors, legislators, regulators, customers, employees, analysts, and consumers. It is the organization's driving value and managing performance expectations for governance, ethics, risk management, and compliance. The key business processes include strategy, operation planning and risk management, performance measurements, and monitoring. Corporate governance is setting and monitoring objectives, tones, policies, risk appetite, accountability, and performance.

ii) Transaction - Level Controls

COSO popularly advices this system on internal accounting control, also called internal control. Some of the basic components of transaction-level controls include (1) control environment (philosophy), (2) risk assessment, (3) control activities include segregation of duties (SoD) authorizations, verifications, reconciliations, and (4) monitoring performance at least annually. Some of the examples of such control processes include (1) master data files of customers, vendors, and employees, (2) disbursement approval, (3) write-off approval, (4) revenue recognition, (5) inventory control, (6) SoD, (7) Information Systems (IS) access, (8) timely reconciliations, (9) cash management, and (10) top level review of actual performance versus budgets or forecasts, and competitors.

iii) Retrospective Examination

The auditing process is an antonym of retrospective examination. The process forms a key link in communicating intolerance for fraud and discovering problems before they grow in size that can threaten the organization. The main objective of ‘generally accepted Auditing Standards’ (GAAS) audit is to form an opinion on the overall financial statements taken as a whole, and the purpose is to serve third-party users of financial statements. GAAS audit adds credibility to reported financial information. Sources of evidence are inquiry, observation, examination, and performance of accounting transactions to support financial statement assertions, and its sufficiency lies in reasonable assurance.

iv) Investigation and Remediation

Forensic accounting investigators respond to evidence, allegations, or suspicions of fraud. They aid auditors to formulate plan like whistleblower allegations. The main objective of Forensic Accounting Investigation is to determine the likelihood and/or magnitude of fraud occurring, and the purpose is to provide sufficient predication that a fraud has or may have occurred. It adds value by resolving suspicions and accusations; and determines the facts. Sources of evidence are review of detailed financial and non-financial data, search public: records, conduct fact-finding as well as admission-seeking interviews, including third-party inquiries, and its sufficiency lies in establishing facts to support or relieve suspicions or accusations." (Appendix)

b) A Fraud Alarm – Whistleblowing

"Whistle-blowing basically means that an employee with knowledge of fraud informs about it to those with the appropriate internal or external remedial authority such as members of management not involved in the fraud, the board of directors, audit committees, internal auditors, external auditors, or outside regulatory and law enforcement bodies, such as the U.S. Securities and Exchange Commission (SEC)" (Rezaee 2002). A Model of the Whistle-Blowing Process (Hooks et al. 1994) must be in the context of the internal and external audit functions that must try to prevent and detect financial statement fraud. Graham (1986) and Miceli and Near (1992) tried to depict the whistle-blowing control chart (appendix) and activities involved in three distinct steps of recognition, assessment and assumption of responsibility, and choice of action. The integrated fraud risk management, as stated by Pickett (2002) enlists some of the stages of the author's model for assessing organizations:

- Board
- Chief Executive Officer (CEO)
- Stakeholders
- Antifraud Mission
- Fraud Panel
- External and Internal Audit
- Ethical Standards Committee
- Audit Committee
- Chief Fraud Advisor / Compliance Office

- Fraud Risk Management Strategy
- Fraud Investigation Strategy
- Fraud Hot Line
- Staff Discipline
- Investigators
- Management
- All other employees

c) Types of Financial Frauds

The recent 'Statement of Auditing Standards' (SAS) No. 99, entitled 'Consideration of Fraud in a Financial Statement Audit', issued by the 'Auditing Standards Board' (ASB), defines two types of misstatements relevant to an audit of financial statements and auditors' consideration of fraud. The first type is misstatements arising from fraudulent financial reporting, which are defined as "intentional misstatements or omissions of amounts or disclosures in financial statements designed to deceive financial statement users." The second type is misstatements arising from misappropriation of assets, like theft or defalcation (AICPA 2002).

Gerson et al. (2004) figured out that earnings management, including intentionally recognizing or measuring transactions and other events in the wrong accounting period, or recording fictitious transactions constituted fraud in Public Company Accounting Oversight Board (PCAOB) terminology. Gerson further explained – "if there is an unusual right -of- return privilege and there is no basis for estimating the returns that will take place, the transaction essentially becomes a conditional sale, and recognizing the revenue when the product is shipped violates 'generally accepted accounting principles' (GAAP) and misstates the financial statements. If the right-of-return privilege has been concealed from the auditor as part of a scheme to increase reported earnings, the financial statement misstatement involves fraudulent financial reporting in revenue recognition." Some examples of combinations where financial statements include transactions or values that are incorrect are in the table below-

Table 3: Misstatements Combination by Dooley & Skalak (2004)

Assets or Liabilities -	Income Statement Effect -
Accounts Receivable [Overstated]	Revenue [Overstated]
Allowance for Sales Returns [Understated]	Revenue [Overstated]
Doubtful Accounts Allowance [Understated]	Bad Debt Expense [Understated]

Inventory [Overstated]	Cost of Goods Sold [Understated]
Inventory Reserves (for Lower-of-Cost-or-Market Impairment) [Understated]	Cost of Goods Sold [Understated]
Inventory [Overstated]	Direct Expenses [Understated]
Prepaid or Deferred Assets [Overstated]	Direct, Indirect or Selling, General and Administrative Expenses [Understated]
Accounts Payable, or Accrued Liabilities, or Other Obligations [Understated]	Expenses [Understated]

The following is an assimilation of different kinds of frauds originally written by Wells (2005) spanning through several pages in a book that contain brief definitions:

- **Skimming** – theft of cash prior to its entry into the accounting system. Sales skimming involve theft of sales receipts, as opposed to payments on accounts receivable. Receivables skimming involve theft of incoming payments on accounts receivable and is much harder to detect.
- **Cash Larceny** – theft of an organization's cash after its recording in the accounting system, which includes receipts scheme and fraudulent disbursements of cash.
- **Billing Schemes** – a scheme in which a fraudster causes the victim organization to issue a fraudulent payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.
- **Check Tampering** – a type of fraudulent disbursement that occurs when an employee converts an organization's funds by either (1) fraudulently preparing a check drawn o the organization's account for his own benefit, or (2) intercepting a check drawn on the organization's account that is intended for a third party and converting that check to his own benefit.
- **Payroll schemes** – form of fraudulent disbursement in which an organization makes a payment to an individual who either works for the organization or claims to work for the organization. Payroll schemes fall into three categories: (1) ghost employees, (2) falsified hours and salary, and (3) commission schemes.
- **Expense reimbursement schemes** – a scheme where employees make false claims for reimbursements of fictitious or inflated business expenses, by mischaracterizing personal expenses, and overstating actual business expenses.
- **Register disbursement schemes** – two basic schemes that take place at a cash register: false refunds and false voids.
- **Non-Cash Assets** – misuse, unconcealed larceny, asset requisition and transfers, purchasing and receiving schemes, and fraudulent shipments.
- **Corruption schemes** are broken down into four categories: bribery, illegal gratuities, economic extortions, and conflicts of interest

"Ponzi schemes may involve multiple pledging of assets claimed to be security for the investors' loans or other investments, commingling of funds and diversion of cash collateral, and fraud in the inducement to invest by mischaracterizing by overstating anticipated returns and misstating the security backing up the investment, and concealing loss risks associated with, the investment. Bank frauds depend on this concept" (Dooley & Skalak 2004). Pickett (2002) also mentions credit-card fraud, consumer fraud, identification fraud, and computer related crime as some of the other common types of fraud.

2) Corporate Governance – Major Deterrence Leaders

"Corporate governance is defined as the mechanism of managing, directing, and monitoring a corporation's business to create shareholder value. Corporate governance is viewed as interactions among participants in managerial functions (e.g., management), oversight functions (e.g., the board of directors and audit committee), audit functions (e.g. internal auditors and external auditors), monitoring functions (e.g., the SEC, standard setters, regulators), and user functions (e.g., investors, creditors, and other stakeholders) in the governance system of corporations. Corporate governance should monitor the interests of investors and creditors by (1) assessing the risk associated with their capital investments in the company resources; (2) evaluating the allocation of their investment for maximum returns; and (3) continuously monitoring the administration of their investments" (Rezaee 2002).

Blue Ribbon Committee (BRC) (1999) revealed, "open communication for oversight in the financial reporting process of publicly traded companies will reduce instances of financial statement fraud which can diminish investors' confidence in the capital markets."

Skalak et al. (2004) stated "some of the key elements of effective corporate governance. The key elements of corporate governance are:

- ❑ An independent board composed of a majority of directors who have no material relationship with the company
- ❑ An independent chairperson of the board or an independent lead director
- ❑ An audit committee that actively maintains relationships with internal and external auditors
- ❑ An audit committee that includes at least one member who has financial expertise, with all members being financially literate
- ❑ An audit committee that has the authority to retain its own advisers and launch investigations as it deems necessary
- ❑ Nominating and compensation committees composed of independent directors
- ❑ A compensation committee that understands whether it provides particularly lucrative incentives that may encourage improper financial reporting practices or other behavior that goes near or over the line
- ❑ Board and committee meetings regularly held without management but in the presence of the CEO
- ❑ Explicit ethical commitment ("walking the talk") and a tone at the top that reflects integrity in all respects
- ❑ Prompt and appropriate investigation of alleged improprieties
- ❑ Internally publicized enforcement of policies on a "no exception" or "zero tolerance" basis
- ❑ The board and/or audit committee's reinforcement of the importance of consistent disciplinary action of individuals found to have committed fraud
- ❑ Timely and balanced disclosure of material events concerning the company

- ❑ A properly administered hotline or other reporting channels, independent of management
- ❑ An internal audit function that reports directly to the audit committee out fear of being "edited" by management (CEO, Chief Financial Officer (CFO), controller, etc)
- ❑ Budgeting and forecasting controls
- ❑ Clear and formal policies and procedures, updated in a timely manner as needed
- ❑ Well-defined financial approval authorities and limits for different professionals
- ❑ Timely and complete information flow to the board”

a) Board of Directors

Rezaee (2002) inducted a summary of the Dey Report, which proposed fourteen guidelines for corporate governance primarily aimed at the activities of the board of directors. “Toronto Stock Exchange (TSE) - listed companies should report on their corporate governance system and on whether their system is in compliance with the guidelines. These guidelines are primarily aimed at the board of directors by (1) specifying the responsibility of the board of directors in the areas of strategic planning, risk management, and internal control; (2) suggesting that the board of directors should be constituted with a majority of unrelated (independent) directors; (3) disclosing whether the majority of board members are unrelated; and (4) discussing orientation and training for new board members, compensation committees, and their functions” (Toronto Stock Exchange (TSE) 1994TSE).

“The separation of ownership and control in corporations requires the board of directors to (1) harmonize manager-shareholder (agency) conflicts of interest; (2) safeguard invested capital; (3) approve management decisions; (4) assess managerial performance; and (5) allocate rewards in manners that encourage shareholder value creation. Management, through its power to nominate or even select directors, can dominate the board of directors and diminish the effectiveness of the board's responsibility in monitoring management. The board of directors delegates its decision-making authority to management, which makes decisions on a day-to-day basis on behalf of shareholders who elect directors. The board of directors usually retains decision control and monitoring function by (1) monitoring managerial decision functions; (2) overseeing the adequacy and effectiveness of internal control system; (3) overseeing the effectiveness of audit functions; and (4) overseeing the integrity, reliability, and quality of the financial reporting process" (Rezaee 2002).

"The review of corporate governance literature indicates that (1) the board of directors is composed of fewer "outside" members for fraud firms than for nonfraud firms; (2) outside members of the board of directors of fraud firms are of lower "quality" than outside directors of nonfraud firms; (3) members of the board of directors of fraud firms hold larger ownership stakes than directors of nonfraud firms; (4) managers (inside members) who serve on the board of directors have higher ownership stakes in fraud firms than managers of nonfraud firms; (5) the chairperson of the board of directors holds a managerial position (e.g., CEO, president) more often for fraud firms than for nonfraud firms; (6) the CEO's tenure on the board of directors for fraud firms is longer than for nonfraud firms; and (7) the average outside director tenure on the board of directors is shorter for fraud firms than for nonfraud firms" (Beasley 1998).

b) The Audit Committee

The Treadway Commission recognized that audit committees play an important role in preventing and detecting fraud. The rules by the SEC, NYSE, AMEX, and NASDAQ improved the effectiveness of audit committee's oversight functions pertaining to corporate governance, the financial reporting process, the internal control structure, and audit functions to deter fraud. "The following are some of the fraud prevention and detection tips for audit committees:

- ❑ Evaluate management's assessment of the significance and likelihood of fraud risks, especially the pressure to meet earnings expectations or creative accounting.
- ❑ Evaluate the internal control best practices that address each fraud risk.
- ❑ Evaluate internal auditors' testing of the effectiveness of each fraud control with full resources at their disposal and adequate communication.
- ❑ Ensure period use of a research-based tool to measure the effectiveness of the CEO's efforts to create the right tone at the top to promote ethical behavior and deter wrongdoing.
- ❑ Ensure that internal auditors continually conduct fraud detection tests using the latest computer-assisted methods, or for large companies, attach a "fraud sentinel" to computer system to detect potentially fraudulent transactions on a real-time basis.
- ❑ Have independent auditors and fraud specialists critically evaluate the results of these items" (Bishop 2000).

c) Management

Management is responsible for first line of defense against fraud for properly constructed system of corporate governance, risk management, and internal control (Skalak et al. 2004). Rezaee (2002) confirmed, “management is responsible for producing financial statements free of material misstatements caused by errors and fraud. Management may be motivated to engage in financial statement fraud because its personal well-being is so closely associated with the well-being of the company through profit-sharing, stock-based compensation plans, and other bonuses: and management is willing to take personal risks for corporate benefits; however, financial statement fraud can be prevented and detected when a company's financial reporting process is subject to thorough scrutiny by the board of directors, the audit committee, internal auditors, external auditors, and governing bodies. Nevertheless, the presence of a ‘gamesmanship’ environment enables management to use its discretion to choose accounting practices that portray the rosiest earnings projections to meet analysts' forecasts to sustain or boost stock prices.” Rezaee also quoted a working paper (Holmes et al. 2000) that “examined the relationships between management attitude and specific dimensions of fraud schemes by comparing frauds that were uncovered in organizations where management had implemented and supported internal control systems (SUPPORTIVE) with frauds that occurred in organizations where management was perceived to display a lax altitude towards internal controls (LAX).

> The study attempted to provide answers to the following three simple but important financial statement fraud-related questions:
>
> > (a) Does the relationship of the fraud perpetrator to the victim entity differ between SUPPORTIVE organizations and LAX organizations? (b) Does the nature of the fraud schemes used to commit the crime differ between SUPPORTIVE organizations and LAX organizations? (c) Does the method of fraud detection differ between SUPPORTIVE organizations and LAX organizations?
>
> It was found that (1) employees were more likely to be the perpetrator of fraud in organizations where management displayed a tax attitude toward internal controls; (2) a LAX altitude by top management toward internal controls encourages unethical behavior on the part of employees, which may result in fraudulent financial activities; (3) more red flags were identified in LAX organizations than SUPPORTIVE organizations before the fraud was detected; (4) perpetrators in organizations with lax attitudes were being prosecuted al the same rate and as severely as in organizations that supported internal controls; and (5) LAX organizations were more likely to fine or transfer perpetrators to discourage the frauds to occur” (Holmes et al. 2000).

Earnings Management

Rezaee (2002) conducted his research on earnings management tendencies among managers. He quoted several authors in their respective researches about inter-linking the likelihood of frauds and management's tendencies to inflate earnings. Below are some of his key summaries of the findings of the other authors:

- "Profitable firms with favorable financial results can more easily and feasibly raise funds through financing than can poorly performing firms" (Brealey et al. 1992).
- "Published financial statements and reported accounting information typically influence the perceptions of potential investors regarding earnings potential and the value of the firm. Management has a strong incentive to hide any deliberate earnings management "since greater payoffs obviously accrue to managers whose accounting manipulations go undetected by the parties that would be adversely affected by them." Fraudulent financial reporting is more prevalent when managerial discretion is curtailed and firms have a higher debt-to-equity ratio than nonfraud firms" (DeAngelo 1986).
- "Managers of firms in weak financial condition are more likely to 'window dress' in an attempt to disguise what may be temporary difficulties. Managerial ownership provides incentives for management to increase the value of their ownership interest by fraudulently reporting a better financial performance than otherwise would be reported under GAAP" (Kinney & McDaniel 1989).
- DeChow et al. (1996) investigated "firms subject to accounting enforcement actions by the SEC for alleged violations of GAAP to determine the relationship between earnings management and weaknesses in corporate governance structure and the capital market consequences experienced by firms when the alleged earnings manipulations become visible. The authors found that an important motivation for illegitimate earnings management is a desire to attract external financing at low cost. They also found that firms engaged in illegitimate earnings management are (1) more likely to have boards of directors dominated by management; (2) more likely to have a CEO as chairman of the board of directors; (3) more likely to have a CEO who is also the firm's founder; (4) less likely to have an audit committee; (5) less likely to have an outside blockholder; and (6) more likely to have significantly increased capital costs when violations (illegitimate earnings management) are made public."

Corbett and Clayton (2004) included a research by Prof. Messod D. Beneish, who researched the quantitative differences between public companies for two consecutive years. "The study found that on average, corporations identified as manipulators had significantly larger increases in day sales in receivables, greater deterioration of gross margins and asset quality, higher growth, and larger accruals than nonmanipulators" (Beneish 1999).

d) Auditors: Internal and External

Three fundamental concepts on auditors' work are (1) fraud versus error, (2) reasonable assurance, and (3) materiality. The auditor can inquire about existence of assets, buying costs, estimations, collection values, and final shipment to customers. The auditor's role does not ascertain management's intent in various transactions. Auditors selectively test only target data because of lengthy timing, and the need to perform large number of tests. Second reason is that fraud characteristics can include concealment, falsified documentation, or management's participation for earnings management. Therefore, auditors do not provide absolute assurance. "SAS 99 cautions the auditor not to place exclusive emphases on amounts because misstatements are not immaterial simply because they fall beneath a numerical threshold. Historically, many auditors may have focused on a standard of percent of pretax income (loss) or after-tax income (loss) from continuing operations as the benchmark for materiality" (Gerson et al. 2004).

Gerson et al. (2004) also explained auditors' philosophy. "Effective and high-quality audit process attributes include professional skepticism, knowledge and experience, independence and objectivity. A framework that includes elements that should be considered in the auditor's assessment of risk of material misstatement caused by error or fraud: SPADE, which stands for S-Skepticism, P-probing communications, A-analytics, D-documentation, and E-evaluation."

Dooley and Skalak (2004) pointed out that lying to an auditor could also result in criminal sanctions. "Fraud on auditors typically includes some combination of the following elements:

- ❑ Misrepresentations by management and/or employees concerning the nature of transactions, the accounting applied, the absence of accounting irregularities-when in fact such accounting irregularities exist-and adequacy of disclosure
- ❑ Concealment of fraudulent transactions by means of falsification, alteration, and manipulation of documents and accounting records or in some cases, by keeping a separate set of books and records
- ❑ Subornation of collusion to defraud from among management and/or employees, taking the form of silence when in fact these persons have knowledge of the fraudulent activities but do not disclose their knowledge to the auditors, active participation in the fraud by corroborating misrepresentations and/or assisting in

the falsification of books and records, and assistance in the circumvention of internal controls designed to prevent or detect fraud

- Collusion with third parties or other employees of the victim company, in which such parties are aware of irregular transactions but do nothing to prevent them and/or nothing to bring them to the attention of either their auditors or the counterparty's auditors
- Deceptions, including planning the fraud to take advantage of known or anticipated patterns of auditing-such as scope of testing or audit locations-and furnishing false information to auditors in response to their audit inquiries
- Destruction of evidential matter and/or withholding key documents such as side letters"

i) Internal Auditors

"Internal auditors should assist management to (1) assess the soundness of the company's internal control environment in setting the "tone at the top" in creating an environment for high-quality financial reports; (2) ensure that management expectations regarding financial performance (e.g., earnings projections) are realistic; (3) communicate, implement, and enforce corporate established policies, procedures, and codes of conduct to all affected individuals within the company and monitor their compliance with activities designed to prevent and detect financial statement fraud; (4) improve communications in providing management with adequate and reliable information; and (5) monitor the corporate internal control system and make recommendations to improve its effectiveness in preventing and detecting financial statement fraud" (Rezaee 2002).

"Internal auditors' responsibilities for detecting, investigating, and reporting financial statement fraud are to (1) identify symptoms and red flags that indicate that financial statement fraud may have been perpetrated; (2) identify opportunities (e.g., weak internal control, weak audit committee) that may allow financial statement fraud to occur; (3) assess the identified symptoms and opportunities, investigate the possibility of their occurrences, and determine actions necessary to reduce or minimize their likelihood of occurrences; and (4) notify the appropriate individuals with the company–top executives if they are not involved in fraud or, otherwise, the board of directors and its representative audit committee–for further investigation of the possibility of financial statement fraud" (Rezaee 2002).

Thus, most publicly traded companies should have an independent, effective, competent, and respected internal audit function. “The board of directors, audit committee, and top management team should support internal auditors and value their services. External auditors should cooperate and coordinate their audit activities with internal auditors because they know the company, the personnel, the company's business environment and risks, and the internal control structure. Internal auditors should get more involved with the review and audit of financial reporting processes to effectively prevent and detect financial statement fraud.” Internal auditors do not limit services because of time and budget constraints that are particular to the external auditors, and should get more involved in fraud deterrence (Rezaee 2002).

Red Flags

Internal auditors' involvement in the routine activities of the corporation and internal control environment place them in the best position to identify and assess evidence that may signal financial statement fraud. “Possible symptoms of financial frauds are listed in three general categories of (1) organizational structure: (2) financial conditions; and (3) business and industry environments” (Rezaee 2002).

SAS No. 82 (AICPA 1997) identifies categories of risk factors (red flags) mostly related to financial statement fraud and two classes of red flags pertaining to misappropriation of assets. Financial statement fraud red flag categories are those associated with (1) management's characteristics and influence over the control environment; (2) industry conditions; and (3) operating characteristics and financial stability. Red flags pertaining to misappropriation of assets are (1) susceptibility of assets to misappropriation, and (2) controls. SAS No. 82 identifies more than 50 risk factors (red flags) related to financial statement fraud and misappropriation of assets. The following risk factors individually or collectively may be the symptoms of possible financial statement fraud: (1) substantial related-party transactions outside the ordinary course of business or with unaudited entities; (2) material, unusual, or highly complex transactions, especially those close to the end of a reporting period; (3) substantial operations or bank accounts in tax havens for which there is no legitimate business justification; and (4) an organizational structure with a huge degree of complexity that is not warranted.

ii) External Auditors

"Independent auditors' responsibility in a financial audit is to plan and perform the audit to provide reasonable assurance that audited financial statements are free of material misstatements caused by errors or frauds. In effectively fulfilling this responsibility, independent auditors are required to obtain a sufficient understanding of the client's internal control system to plan the audit and determine the nature, timing, and extent of audit test procedures. If the auditor decides to assess control risk below the maximum level, the tests of controls should be performed to determine the effectiveness of the prescribed control activities" (Rezaee 2002). As a matter of commercial reality, "audits are performed in a client-controlled environment. Because the auditor cannot in the time available become an expert in the client's business and record-keeping systems, the client necessarily furnishes the information base for the audit" (Gerson et al. 2004).

In summary, the O'Malley Panel on Audit Effectiveness (Public Oversight Board (POB) 2000POB) stated that the most important determinants of audit effectiveness are the personal attributes and skills of the individual auditors that provide structure and definition for their role in society and their involvement in the financial reporting process.

Aronow et al. (2004) commented on the public responsibility of an independent public accountant - "By certifying the public reports that collectively depict a corporation's financial status a 'Certified Public Accountant' (CPA) owes ultimate allegiance to the corporation's creditors and stockholders. The auditor is quite likely to be the first person to get blames for errors or inadequacies in financial disclosure almost without regard to his or her audit responsibility. They search for a source of funds to correct financial fraud."

iii) Fraud-Specific Auditing Standards

The Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) amended SAS No. 61 with two new

SAS rules: 89 and 90. SAS No. 89 (AICPA 1999) requires external auditors to communicate to the audit committee about misstatements that the management considers unimportant. SAS No. 90 (AICPA 2000) requires auditors to discuss with the audit committees their judgment about the quality, not just the acceptability, of the entity's accounting principles and the estimates underlying the financial statements; and certain matters identified in their quarterly review of interim financial information before it files with the SEC.

SAS 99 Fraud Risk

Auditor's work engagement risk includes litigations, adverse publicity, and lack of payment for services performed, loss of professional reputation, and loss of other clients. SAS 99 provides guidance for auditors concerning how to apply a risk based approach to the possibility of fraud by measuring internal control risks and management override of controls. SAS 99 sets out three areas that require substantive procedures that address the risk of management override: journal entries and other adjustments, accounting estimates, and significant unusual transactions. To address this risk, SAS 99 instructs auditors to perform a retrospective review of past accounting estimates for biases that could result in material misstatement due to fraud. SAS 99 teaches auditors to gain an understanding of the business rationale for all significant transactions that fall outside the normal course of business or otherwise appear to be unusual, given the auditor's understanding of the entity and its environment. In exercising professional skepticism while gathering and evaluating evidence, the auditor should not be satisfied with less-than-persuasive evidence because of a belief that management is honest, and must reassess the corporate environment for fraud each year.

Kenyon & Tilton (2004) broadly described, “some probing and explicit questions about fraud risks and the possibility of fraud as contemplated by SAS 99. Among the topics the auditor might raise with management, the following would be among the most important: knowledge of any fraud or risks of fraud, any letters or communications from associates concerning allegations of fraud, any specific account balances or classes of transactions for which a risk of fraud may be more likely to exist, programs and controls to mitigate specific fraud risks, and communication on business practices and ethical behavior. To the audit committee, the auditor might inquire on assessment of management's performance.” The questions may form the basis of interviews with management and key financial staff.

Table 4: Interviewing and Fraud Risks by Kenyon & Tilton (2004)

Questions on Pressure to meet Budget & Fraud Risks
Sample Questions for Management:
How were goals and/or budgets achieved during a down economy? What did your company do differently from its competitors to obtain revenue or earnings-per-share goals when the rest of the industry was not meeting expectations? Were any changes implemented during the quarter so that goals and/or budgets could be achieved? For example, were new customers obtained or were cost-cutting measures implemented? What specifically caused the company to meet goals and/or budgets?
Sample Questions for Financial Staff:
Do you ever feel pressured to maintain the books and records with an eye toward managing actual expenses or revenues to be in line with budgeted expenses or revenues? It is also generally advisable to probe management and other financial staff regarding the overall ethical environment of the organization. Does a written code of ethics exist? Are top managers and employees required to periodically confirm that they comply with the code of ethics? Do top managers and employees receive training in the code of ethics? Have disciplinary actions been taken related to violations of the code?
Fraud Risks Indicative of Material Misstatements-
□ Factors related to the nature of the industry in which the entity operates: the nature of the entity's business and the transactions, and the manner in which they are recorded in the profit-and-loss account or balance sheet. □ The nature of the entity's relationships with customers and suppliers and its position in its markets: the ability to dominate or dictate terms may create the opportunity for inappropriate or non-arm's-length transactions. □ The degree of judgment involved in determining the level of income or expenditure or the valuation of assets or liabilities: Generally, a higher degree of judgment will give rise to a greater opportunity for deliberate manipulation.
Fraud Risks on the Intangible types of functions-
□ Risk factors in an intangible but critically important category include: □ Lack of clarity or communication about corporate ethical values or infrequent communication and reinforcement of such values □ Disregard for the risk of fraud–or ineffective measures when fraud rises □ Lack of realism in budgeting and forecasting and in communicating expectations to third parties □ Recurring attempts by management to justify inappropriate accounting or disclosure policies and practices on grounds of materiality or other grounds □ Difficult relationships with the entity's auditors: a bullying attitude, imposition of unreasonable time pressure, or constraints on access to relevant audit evidence.

iv) Auditor’s Financial Analytic Techniques

Kenyon & Tilton (2004) described various analytical techniques to deter financial frauds. The following information is contributed by the authors to integrate financial analysis:

“Using analytic procedures, auditors develop expectations for actual financial amounts, ratios, trends, and relationships based on their prior experience of the company (modified to reflect any known factors expected to change the outcome), experience of the relevant industry or of similar companies in the industry, expectations of management at the outset of the reporting period, and the actual operational activities of the company. Therefore, the following comparisons are typical aspects of analytic procedures, besides regular financial statement analysis techniques:

- Current company data versus company data from prior period
- Company data versus company budgets, forecasts, or projections
- Company data versus industry data and/or comparable company data
- Company financial data versus company operational data such as production levels, number of employees, and square footage
- Subset of company data versus other subset of company data: comparison of data on a disaggregated basis such as by division, product, location, or employee
- Company data versus auditor-determined expected results

In addition to standard ratios, it is also relevant to analyze other relationships involving the high-risk areas of revenue recognition and inventory balances. Relationships that can be analyzed in these categories might include the following:

- Sales versus sales commissions
- Sales versus returns, allowances, and discounts
- Sales versus advertising or promotion budget
- Sales versus outbound freight costs
- Sales versus cost of sales
- Sales versus accounts payable
- Sales versus gross profit
- Sales versus inventory
- Sales versus production levels/capacity
- Sales versus measure of total market size
- Sales versus accounts receivable
- Sales versus interest expense
- Inventory versus cost of sales
- Inventory versus current or total assets
- Inventory versus production levels

Finally, analysis of relationships that involve cash or cash flow can reveal areas requiring further review. The cash account is rarely misstated because of the ease with which cash balances can be confirmed. Therefore, examining the relationship between cash–which is likely to be stated properly–and other account balances that might be misstated can identify anomalies" (Kenyon & Tilton 2004).

3) Forensic Financial Services

For the purpose of the thesis, the roles of forensic accountants, forensic technologists, and forensic accounting investigators are essential for explaining the internal control necessities. Forensic technologists are also known as investigative data analysts with very strong technical and communication skills. Forensic accountants can focus on commercial disputes in specific industries or a wide range practice areas, such as construction, environmental issues, intellectual property, government contracting, insurance and business interruption, marital dissolution, shareholder litigation, business valuation, business combinations, and cybercrime. However, this thesis emphasizes only fraud deterrence, which puts more importance to the investigating role of the forensic accounting investigator.

a) Forensic Accounting Investigators and External Auditors

Cooperation Efforts: Auditors and forensic accounting investigators share responsibility of work, if an investigation must commence. A detailed outline of their cooperation is depicted by Skalak & Golden (2004) as shown below:

In the United States, “the forensic accounting investigators may neither take direction from client's counsel nor aid client's counsel in any manner typical of consultants or expert witnesses working on behalf of the company. Auditors and their forensic accounting investigators are precluded from an advocacy role on behalf of clients – however minimal the role might be. On the other hand, they may share their planned investigative and other audit procedures, as well as their findings, with the client and client's counsel at the direction of the audit committee or special committee charged with overseeing the investigation. Nonetheless, the auditing firm's forensic accounting investigators must be careful not to cross the line between the permitted, expanded audit scope and the prohibited expert services.” The following adapted table summarizes allowed and prohibited forensic accounting services and fact-finding engagements under Sarbanes-Oxley:

Table 5: Investigator's Involvement by Skalak & Golden (2004)

	Services Rendered in Defense of Enforcement Agency Investigation	Services Provided as an Extension of Audit Scope to Assist Current Auditors	Providing Expert or Consulting Services under a Legal Privilege	Assisting Audit Committee with Internal Investigation of Potential Accounting

				Impropriety
Non-audit Client	Allowed	Allowed	Allowed	Allowed
Audit Client	Prohibited	Allowed	Prohibited	Allowed

“It is not permitted for this assistance to include defending or helping to defend the audit committee, or the company in shareholder class action or derivative lawsuit, or an investigation commenced by a governmental enforcement agency, unless begun prior to an enforcement proceeding. Witness services are permitted in court cases” (Skalak & Golden 2004).

Difference in Roles: A cross-comparison between forensic accounting investigator and auditors can peculiarly demonstrate some of aspects of different working atmosphere among these professionals as staged by Ranallo (2004):

> “Forensic accounting investigation explicitly does not involve financial statements but focuses on evaluation of transactions, people or business units to determine whether there are perceived problems that require further actions. Forensic accounting investigators serve the interests of the party that engaged them. The overall focus of their activity may be set by a committee of a company's board of directors, by counsel, or by senior managements. On this basis, they propose a plan and generally seek agreement that its proposed scope address the issues of concern. As the inquiry begins and findings become known, the investigation is often shaped by instinct and judgment calls, and the initial plan evolves. Rarely is there a relevant base of prior work to draw upon.
>
> Auditors, in contrast, set the scope of the audit, based on risk factors determined after consideration of relevant information, including books and records, management input, and other data such as industry norms. The auditors benefit from cumulative knowledge based on prior work and advance planning. While the auditor places at least some reliance on management representations, the forensic accounting investigator usually places little or no specific reliance on management representations. The task of the forensic accounting investigator is often to evaluate the reasonableness of management positions.
>
> A sharp contrast exists in how sampling is used for accomplishing various goals in the two related but distinct disciplines. On one hand, auditors may use attributes sampling to test compliance with internal control procedures or may use variables sampling to test the dollar amount of errors or estimate a population value from sampling techniques. They may test all large transactions accounts. Forensic accounting investigators, however, are more likely to use discovery-sampling techniques, which allow for quantification of the likelihood of finding one specified condition in a population. They may use sampling in proportion to size–also called *dollar-interval sampling*–to estimate the upper limit of a population value. In addition, they may examine all transactions in a relevant period that meet a particular profile, such as all transactions approved by a certain responsible person, all transactions with a specific third party, or all transactions of an unusual dollar amount. Data mining, including e-mail review, can examine the entirety of a vast set of transactions and communications.
>
> Auditors must work without indemnification protection: the SEC prohibits such arrangements. Forensic accounting investigators, however, usually have both indemnification and hold-harmless protections because of the use made of third-party information, the contentiousness of the issues covered by the forensic report, and the fact that they do not control the scope of their work” (Ranallo 2004).

b) Forensic Accounting Investigator and Attorneys

According to Golden et al. (2004), “forensic accounting investigators can expect to work with or for attorneys in internal investigations with respect to accounting or reporting matters. The number and kinds of attorneys are broad and varied. The forensic accounting investigator may work with the special independent (external) counsel to the board of directors or the audit committee, attorneys for specific board or audit committee members, and counsel for specific employees or groups of employees. When potentially material accounting irregularities – or allegations of potentially material fraud– come to its attention, the board of directors typically seeks the advice of counsel on a number of considerations that may include informing audit committees, stakeholders, and setting up an investigating team after stabilizing data and security.

The investigating team often includes independent counsel, Forensic accounting investigators, Forensic technology experts, External auditor partner, and key staff. Based on the specifics of the investigation, the team may include other experts or specialists such as engineers, actuaries, tax experts, investment bankers, valuation or appraisal specialists, and damages experts. Independent counsel, with the help of forensic accounting investigators, often takes the lead in setting up, organizing, and managing the investigative team. This process may include the selection and retention of other parties who make up the team. The forensic accounting investigator can expect to work with or for attorneys in most investigations. To help ensure that the investigation progresses as smoothly as possible and reach appropriate conclusions and satisfactory resolutions, each member of the investigating team should collaborate intelligently” (Golden et al. 2004).

Summary:

The chapter has answered the questions on the roles of corporate governance and forensic accounting services in deterring fraud. This chapter includes the description of the fraud deterrence cycle, which guides the thesis results in defining transaction-level controls, because it sets the focus of the thesis.

Chapter Four

❖ *Empirical Results*

This chapter presents the results of the document reviews. As explained in the problem statements, the chapter asserts on most popular technology used by professionals, kinds of software, and internal control business processes. This chapter includes three subsections for the remaining problem statements. The first subsection uses coding and grouping of contents from the methodology chapter. After describing items in codes, it becomes essential to describe each kind of software and different internal control templates from company X in consecutive subsections.

1) Suitable Fraud Deterrence Software [♣]

Some software specifically detect fraud ([FD] & [F]), which integrates with most data-mining software used by forensic accounting investigators, however, actual control implementation [A] does not relate with fraud detection software. Transaction-level controls include planning and budgeting, which is available through dashboards and data analytics ([BI] & [PM], but insignificant [F], or possible use in [A]). Furthermore, risk assessment requires setting up of audit trails and efficient data management of business processes ([C], [DM], [P] and preventive [F] with notable impact to routines in [A]). However, as increasing use of fraud detection technology in online payments suggests, internal controls need to stabilize with separate transaction processes, where exchange of funds occurs ([ERP] & [TS], with equivalence to all [A] and possibilities of curbing all [F]). A good example of a popular technology, which integrates several kinds of software, is vendor

[♣] View Codes on Page # 10 - 11 and review methodology for data on company X processes

ACL, which offers continuous monitoring solutions. Ideally, it offers one of the most popular software suites (includes [C], [DM], [FD], [TS], with some compatibilities with [ERP] & [A], and simple use of other software kinds with full scope to deter [F]). SAP and Oracle, which are ERPs also display transaction transparency because of constant integration of data throughout the enterprise.

Therefore, the constant comparison method yields an answer from the sample of chosen firms; ACL and SAP have the widest range of acceptability in deterring fraud. The field memos on ERP and transaction systems are available in the next two section of this chapter. This adds affirmative status to the original hypothesis test of the methodology chapter, if taken positively, because it seems logical that fraud risks are lesser on the transaction-level itself, where transaction system or ERP software assures the reported amounts are correct, and made by authorized personnel in the right accounting period. However, the technology must not be only a generic software solution, but more focused on COSO agenda-based continuous monitoring software that conducts constant data mining and audit trails for noticing any deviations, and alerts the staff of inaccurate entries that can broadly deter fraud before it gains momentum.

2) Software Criteria

An internet article by Bruce Winters (2004) on internal control reporting software tools set the criteria of kinds of software and names of possible firms. The document explains the categories of most popular software dedicated to effective internal control reporting. The article is comprehensive and analyzes software with external links to vendor software firms. It highlights the need of correct software selection to reduce costs and get necessary tools that CPA firms must consider before consultation with the client firm. For this essay, the article gives a brief insight on kinds of software that ensure internal control and reduce fraud. This section further depicts added subdivisions to the listing.

a) A Generic Accounting Application - SAP

The information from company X explicitly mentions MS-Excel, SAP, and firm’s (own) legacy software for implementing various transactions. This limits the generic software vendor listing to only SAP, Most of the accounting and finance professionals must have experienced knowledge into ERPs like SAP, while using software.

SAP is an ERP system, which means that it links data in real time across the traditional business functions with flexible configuration, but complex authorization profile. The role of SAP and emphasis on accurate business processes has challenged the middle management’s role in collating and reporting, review and authorization, which SAP and other ERP systems replaced. Most of the basic controls are similar to transaction systems, and all processes have description in the company X internal controls data. Other auditing areas include master file control, user management, and specific validation checks in particular transactions.

Fraud auditing in SAP depends on document types for manual querying by ‘general ledger’ (GL) accounts. In-built Accounts Payable functions mostly use the principle of using particular codes only once within the system. ‘Segregation of duties’ (SoD) is possible through identification of users with incompatible duties such as purchasing, goods receiving, invoice processing, and cash payments. Accounts Payable (AP) also requires that organization processes payments based on relevant transaction codes for each step, key control points, and SoD. “SAP can provide some powerful accounting authorizations to the internal auditors, such as all assets accounting profile, maintenance for fixed assets, payment transfers, and process manufacturing. SAP can be both a means to cause fraud and a useful tool in curbing frauds. Most significant user based fraud risk is system access and authorization” (Moulton 2002).

For fraud detection, “SAP R/3 provides security audit logs, changes in master records and accounting audit trails. The SAP method comprises of two stages: (1) threat watching, which involves high-level surveillance of security audit logs for threatening signs of fraud, and (2) automated extraction and analysis of data from audit trails to provide documentation of user actions.

Forensic investigation can then determine whether fraud has in fact been perpetrated" (Best 2005).

b) Business Intelligence (BI)

"Business Intelligence tools make it possible to examine the results of business operations, delving deep into data and adjusting items to see how they affect a financial calculation. It also enables users to review data for patterns, and with the arrival of tools that are easier to connect to financial systems, this kind of software also has become cost-effective" (Winters 2004).

The scope of analysis for BI software is extensive, but vendors enlist distinctive skills within this category. There are many instances, where this kind of software has similar qualities to other internal control software products. When conducting document review for BI software, some features were prominent:

- Data warehouse reporting with query
- Graphical reports, dashboards, grids and charts
- Loss prevention by analyzing payment transactions
- Monitor operational systems to detect business process events
- Alerts to deliver time-critical information to decision-makers

(Grouping of BI features obtained from corporate sites of Hyperion, Cognos, and BusinessObjects 2007)

The vendors, Hyperion and Cognos actively promoted database filtering, special query, reporting, and dashboards. Hyperion's software can file financial statements electronically in 'eXtensible Business Reporting Language' (XBRL) format. Cognos added strategy maps metrics and alerts for decision making that could help corporate governance members when necessary. BusinessObjects mentioned that analytics provided by BI software was useful to the retailers for 'point of sale' (PoS) and payment transactions, and to alert managers of any suspicious behavior. A comment explains,- *"High bandwidth connectivity to stores and advanced analytic systems are identifying fraud and theft as they happen - and immediately alerting loss prevention staff to take corrective action"* – BusinessObjects 2007

c) Compliance

According to Winters (2004), "real-time compliance tools store all information in one 'data warehouse' provide consistent and efficient processing, timeliness and accuracy, include rapid warning and response systems and make it easier to monitor and manage risks. These tools also provide performance management and workflow roles.” Some of the central features of this software are in the following grouping:

- Complete audit attestation-ready control documentation
- Manage document lifecycle until archive
- Reports, surveys and dashboards for visibility
- Easy access for auditor walkthroughs of chosen accounts
- Governance-related communication
- Secure data storage with managed user access-
- Audit management for risk assessment and inclusive steps
- Independent risk evaluation of process structure-
- Risk-based compliance of decentralized activities
- Automated workflow of responsibilities
- COSO and SAS 70 document management
- Valid period-to-period comparatives
- Audit logs to track changes to, plans or tests-
- Web-based assignment and access to assigned tasks-
- Monitor workflow by e-mail, attachments and instant messages-
- Evaluate account balances to classify controls that need testing

(Grouping of Compliance features obtained from corporate sites of Certus, Paisley, Axentis Enterprise (Ae), BusinessObjects, Handysoft BizFlow, IBM, and Movaris 2007)

Certus is a major contributor to the compliance software grouping, with six works, followed sequentially by two features from Paisley, five features from Axentis Enterprise, and one each from Handysoft, ‘International Business Machines’ (IBM), and Movaris. Certus allowed auditor walkthroughs, and Axentis Enterprise stressed process centered oversight management for overall company BI efforts by which executive management and boards of directors can achieve critical visibility and defensive audit trails. IBM suggested its DB2 content manager, SOX Web Services, and SOX module hierarchy for executives to configure audit control, enterprise security, change management, workflows, business process management, and project collaboration. Movaris offers compliance software specifically for section 404, 406, and 302 of SOX.

d) Data Management and Workflow

The data management tools interact with other software that is generic products, monitor workflows, and processes to make them more event-driven, and thus easier to manage. "Companies using these tools can better understand and analyze the frequency of internal control procedure, group internal control types, test their effectiveness and reveal relationships between key job responsibilities and their place in the workflow. These tools also analyze risk, controls, and set ranks for importance, materiality, and impact. The tools organize risk and controls by work group in a way that can continually update to suit with changing business conditions, and offer summaries for quarterly review and management approval" (Winters 2004). Following are the software's grouping of features:

- Easy access to all files by simple search pages and navigation items
- Web-hosted document management service to collaborate with lawyers or partners
- Universal file format or Adobe 'portable document format' (PDF)
- Integration with existing databases
- Document modification audit trail, archive and security in compliance
- Automated e-mail policies for corporate governance requirements
- Automated capture and classification tools for workflow to reduce time
- Manage financial and operational data, metadata, master data, and data quality
- Monitoring of work-in-progress, work-item and workflow processing time, queues and workloads

(Grouping of Data Management and Workflow features obtained from corporate sites of FileNet, eFileCabinet, GoFileRoom, EMC, Hyperion, ACL, and IBM 2007)

Software vendors, GoFileRoom and EMC allow web-based service and are identical in configurations. EMC provides added e-mail and lessened workload with automated capture and classification. However, GoFileRoom provides integration with existing databases, such as billing or vendors. eFileCabinet is a desktop-based solution, which can run on a single machine. FileNet provides a process analyzer dedicated to workflow software solutions, which conducts real-time monitoring of total objects in a particular step in the process, displays processing time and number of work-objects in inbox, and provides the capacity to view the total number of launched, completed and in-progress workflows during a named period. A highlighted comment state-

> *"Using multitable, the solution also allows users and managers within the company's sales, service, and accounting departments to make better decisions regarding marketing, improve customer service, and reduces billing errors." - ACL 2007*

e) Fraud Detection

The following is a brief listing of works performed by fraud detection software:

- Strong reconciliation controls for bank, savings, loans and building society systems
- Dormant accounts, revolving loans and money laundering
- Detection in several data files – vendors, buying, and more
- Automatic internal controls testing of independent transactions for inefficiencies
- Automated, predefined analytics to critical control processes
- Identity-based confirmation of multiple identities and accounts
- Trend analysis for accuracy including whistle-blower systems and surveys

(Grouping of Fraud Detection features obtained from corporate sites of IDEA, ACL, BusinessObjects, IBM, and Axentis Enterprise 2007)

The vendors chosen from the stated internal reporting tools article were IDEA, ACL, BusinessObjects, IBM, and Axentis Enterprise. IDEA provides users with stand-alone software system. On the contrary, ACL (2007) has the most dynamic solution to “conduct antifraud analytics within core business processes that represent high risk areas to the organization by quickly identifying suspicious transactions that may represent fraud, error, and abuse, and closing control loopholes before fraud intensifies. Skilled auditors and fraud investigators use ACL, because its technology can access and analyze unlimited volumes of data from almost any enterprise application. ACL ‘Continuous Controls Monitoring’ (CCM) solutions identify fraud, errors, and inefficiencies, by automating internal controls testing in key financial and operational processes across the enterprise through independent analysis of business transactions.” For more variety, IBM provides identity-based verification, and Axentis Enterprise offers incident detection tools.

f) Business Performance Management (BPM)

“BPM tools add continuous auditing competence to real-time enterprise systems in the form of customized computer screens—called dashboards—that present key performance indicators managers use to react to changing business conditions. These tools can smoothly interact with other software and systems and provide one repository for all company information, simplify the development of consistent and more efficient processes, help optimize information timeliness and accuracy, and notify management of compliance problems and solutions" (Winters 2004). The following are the key features:

- Budgeting, planning, forecasting and reporting
- Early warning alerts for real-time collaboration
- Audit trails for future analysis

(Grouping of Business Performance Management features obtained from corporate sites Cognos, Extensity, and BusinessObjects 2007)

The vendors for this category were Cognos, Extensity, and BusinessObjects. Cognos (2007) states, "Scorecarding, dashboards, and financial consolidation systems supply the metrics to answer 'How are we doing?' Reporting and analysis applications explain the 'Why?' And planning, budgeting, and forecasting systems look forward to tell the organization the answer to 'What should we be doing?'" Extensity summarizes the value of its software as a tool relevant for budgeting, forecasting, planning, and reporting. BusinessObjects uses alert and audit trail for measuring performance.

g) Business Process Management

BizFlow Process Studio (BPS) integrates traditional BizFlow design and management components, such as Process Designer, Process Analyzer, Forms Designer, and Organizational Manager, to create a single collaborative environment, with extra features such as project team support and resource sharing across multiple projects. Metastorm stimulates and models process changes based on real process data from process database *(grouping of Process Management features by Handysoft and Metastorm 2007).*

h) Transaction Systems

Some of the major transaction systems are alike ERP in core functions. ACL leads the market with wide range of features, such as Purchasing Cards, Purchase-to-Payment Cycle, Travel and Entertainment Expenses, Payroll, Order-to-Cash Cycle, and General Ledger. Besides identifying and preventing error, misuse, and fraud, ACL's Continuous Controls Monitoring (CCM) provides management with greater visibility, much alike vendor Approva, IDEA, Movaris and Extensity that offer workflow automation and transactions capacity, but do not mention continuous monitoring capacity *(grouping of Transaction Systems features by IDEA, ACL, Approva, Movaris, and Extensity 2007).*

This finishes software listing that aid in internal control reporting processes. The data showed bulleted grouping of features for each kind of software that its vendors try to sell to firms. Many vendor corporate sites have description of the features that hold website references later in the thesis. The next subsection targets data from company X.

3) Control Objectives

The data in tables comprise of process controls description from company X in Sweden. Its grouping was according to the company's business processes. There was lesser mention of redundancies in financial reporting risks and internal control practices, but most control objectives were in place for the reader to judge actual process. The financial reporting risks (or fraud risks) are not in the tables for each of the corporation's business processes. Because the processes contain repeated sentences for items like misrepresentations, timely filing, wrong postings, and 'Accounting and reporting guidelines' (A&RG) based on US GAAP. Similarly, the internal control tools and practices included rules for employees, which are not in tables except for underlined depiction of underlying IT roles. The sampling rules are the same as mentioned in the Methodology chapter. Besides the shareholder's equity control process, the Board of Directors rarely took part in any other control processes. The CEO and CFO form an integral part of the processes, and there roles have descriptions in MS-Excel spreadsheets. Following are the tables of internal control processes (Some show financial reporting risks, and IT use):

Table 6: Internal Controls for Accounts Payable

ACCOUNTS PAYABLE
Control Objectives:
☻All amounts posted to the system must represent actual goods/services received with accurate calculation and recording in appropriate accounting period. ☻Any adjustments to accounts payable must be accurately recorded. ☻Cash disbursements and checks must be processed accurately. ☻Facilities for electronic funds transfer must be secured and authorized.
Financial Reporting Risks:
☻In Accounts Payable, matching receipt is missing with incorrect posting of details.

☻Invoices are inaccurately captured with incorrect amounts. ☻Accounting principles are not followed in assigning disclosures for AP, with adjustments made without approval. ☻Amounts reported in multiple places are not consistent, or computations and footings are incorrect. ☻Credit or debit notes are not recorded with necessary accuracy. ☻Maturing payment and cash disbursements information is recorded incorrectly or without prior approval. ☻Cash disbursement is duplicate or to wrong vendor.
Actual Internal Control Tools and Practices:
• SAP report viewer for monthly closing to ensure Supply Manager of goods receipt prior to approval and filing. • Lotus Notes is used for routing authorization logs.

Table 7: Internal Controls on Accruals and Provisions

ACCRUALS AND PROVISIONS
Control Objectives:
☻The control objectives target accrued liabilities and other expenses that must be accounted in accordance with US GAAP rules in full accuracy. ☻Information from other financial processes must be available on time and with full accuracy. ☻All accrued liabilities and expenses must be authorized.
Financial Reporting Risks:
☻All accruals and provisions are either not recorded or have been booked without any actual liability basis in an incorrect accounting period and in an untimely manner. ☻It implies key assumptions for accruals and provisions are not supported by business transactions or facts, are inconsistent with selected accounting principles of the organization. ☻Methods and computations are inconsistent with varying situations. ☻Accruals and provisions are not appropriately authorized.
Actual Internal Control Tools and Practices:
• Accruals and provisions must originate through an estimate or statistics. • Upon verifying supporting documentation for specified accrual accounts, journal entry is initiated. • SAP integration automatically handles costs not yet recorded on delivered orders and close old orders. When an order is invoiced, SAP compares pre-calculated cost against actual cost, on each order. If pre-calculated cost is higher, the system makes an accrual. • Accrued liabilities get reconciled quarterly for account close and are identified in general ledger accounts. • The location of the database A&RG where information on recognition, measurement and valuation of accruals are found is in Lotus Notes.

• Review of the SOD matrix in Excel • During closing process the accounting department finalizes the company's own reporting package (the consolidation and reporting system for the financial package), based on specific accounts in P/L and balance sheet. The reporting package includes reporting lines related to restructuring.

Table 8: Internal Controls for Cash Funds

CASH FUNDS
Control Objectives - Cash Management:
☻Established country / unit cash management policies including those related to short-term securities must be uniformly implemented within individual operating units and records related to bank accounts / agreements must be safeguarded against unauthorized access or use. ☻All bank accounts, including overdraft accounts and deposits / investment accounts must be authorized and properly managed. ☻All cash balances must be pooled timely and accurately, reported and monitored in accordance with Group / country policy. ☻All cash and bank transactions / balances and restricted cash balances must be captured and recorded timely and accurately. ☻Cash handled / held by employees must be safeguarded against theft and fraudulent use.
Control Objectives - Investments:
☻Investments and related documents must be safeguarded and secure. ☻All recorded investments represent valid and owned investments / securities. ☻Short term investment of excess cash, including related investment income, must be authorized, approved and accurately and timely accounted for in accordance with the A&RG. ☻All disclosure information related to short-term investments must be captured accurately and completely for each accounting period.
Actual Internal Control Tools and Practices:
• Cash transactions on accounts in foreign currency are recorded manually in SAP R/3

Table 9: Internal Controls for Commitments & Contingencies

COMMITMENTS AND CONTINGENCIES
Control Objectives - Legal and Litigation:
☻All legal and contractual agreements and commitments must be documented, reviewed, approved and physically secured. ☻Information on litigation and claims, and commitments & contingencies must be accurate and timely. ☻Liabilities arising from legal contingencies must be accurately and completely recorded and disclosed in the financial statements in the appropriate accounting period.
Control Objectives - Environmental:
☻Information related to environmental contingencies must be captured correctly for

the financial accounting & reporting process. ☻Liabilities arising from actual breaches of environmental laws and regulations must be recorded accurately and completely and disclosed in the financial statements in the appropriate accounting period.
Control Objectives - Product Guarantees:
☻Information related to performance guarantees and other product / order related contingencies must be recorded with full accuracy. ☻Liabilities arising from performance guarantees and product / order related contingencies must be recorded accurately and completely and disclosed in the financial statements in the appropriate accounting period.
Control Objectives - Financial Guarantees:
☻Liabilities arising from financial guarantees must be recorded accurately and completely and disclosed in the financial statements in the appropriate accounting period. ☻Information on financial guarantee must be accurate, timely and complete.
Control Objectives - Gain Contingencies:
☻Gain contingencies must be recorded and disclosed in accordance with the A&RG.
Actual Internal Controls Tools:
• Compliance with the ISO 14001 standard (and thus laws and other regulations) is subject to regular internal and external audit.

Table 10: Internal Controls on Financial Reporting

FINANCIAL REPORTING
Control Objectives:
☻Accumulation and presentation of financial information must be ruled by established policies and procedures. ☻Roles and responsibilities in regards to the processing and reporting of financial information must be defined with adequate segregation of duties between different accounting roles, CFOs, and managers. ☻General ledger master data must be accurately administered and all changes must be authorized. ☻General Ledger accounts must be accurate as to amount, time and authorization. ☻Journal entries must be recorded accurately and completely in the appropriate accounting period. ☻Financial statement accounts / balances / disclosures must be valued in accordance with A&RG. ☻Monthly, quarterly and annual closing activities must be defined and coordinated. ☻Where consolidation of units must be required (sub-consolidations), all entities / units requiring consolidation must be included in accordance with the A&RG. ☻All information reported in the monthly, quarterly and annual financial reporting package must be prepared in accordance with reporting instructions, reconciled to local accounting records and reviewed by reporting business unit management (CFO and controller) before submission to Finance and Controlling department. ☻The country CFO assumes full responsibility

for the existence and completeness of all operations and financial reporting system in his / her country. ☻The Finance and Controlling department must cover internal controls over financial reporting in relation to consolidating the financial statements, preparing financial statement disclosures, and reporting to the SEC.

Table 11: Internal Controls on Financial Management

FINANCIAL MANAGEMENT
Control Objectives:
☻The hedging strategy and requirements, and the use of derivatives must be defined and approved by the appropriate level of management and communicated / monitored through the whole company. ☻Only authorized financial products / instruments and derivatives must be used. ☻Only authorized and qualified personnel must be allowed to enter into hedging transactions and / or to use derivative products. ☻Only pre-approved third party counterparts must be dealt with in contracting financial products / instruments and derivatives for hedging transactions. ☻Financial positions and exposures (e.g. foreign exchange (FX) / interest rates (IR) / commodity and other financial exposures, including hedges) must be identified, measured, aggregated, and reported timely and accurately in accordance with financial policy and the A&RG. ☻ A&RG applies to all derivatives, including embedded derivatives. ☻The accounting records must accurately reflect the hedging transactions (income statement, assets and liabilities) / financial exposure. ☻If applicable, there must be on-going monitoring that appropriate internal controls policies and procedures exist at third party service providers to which certain hedging activities have been outsourced.

Table 12: Internal Controls on Intangibles

INTANGIBLES
Control Objectives:
☻All intangibles must be initially recorded at cost and processed accurately in the appropriate accounting period. ☻All intangible acquisitions and disposals recorded in the register must be valid and supported by valid documentation. ☻Ownership of or rights to intangibles must be protected. ☻Amortization charges for intangibles with definite lives must be valid and recorded accurately and in the appropriate period in line with A&RG. ☻Internally generated intangibles must be capitalized accurately, only if they satisfy the capitalization criteria in accordance with the A&RG, such as for internally developed software. ☻Goodwill and indefinite life intangibles must be valued in accordance with the A&RG.

Table 13: Internal Controls for Inventories

INVENTORIES
Control Objectives:

☻Full accuracy must be observed when recording goods and enforcing SOD. ☻Inventory must be safeguarded according to existing records and movements in manufacturing cycle must be fully authorized. ☻Inventory must be accurately recorded at net realizable value. ☻Excess and obsolete inventory and its costs must be valued in accordance with the A&RG. ☻Alternative costing methods (e.g. standard, total absorption, activity based, marginal, job, process or unit costing) must be applied accurately and in accordance with A&RG.

Financial Reporting Risks:

☻All rejected good/services and every receipt were not recorded accurately and in the correct accounting period. ☻Receiving records were generated without a physical receipt of goods / services. ☻Authorization, recording, custody and controlling were inadequately segregated. ☻Inventory data files (i.e. inventory master file) and production programs are not protected from unauthorized access. ☻Adjustments to inventory or consigned inventory records are done inaccurately. ☻Independent inventory counts / confirmations of inventory at outside locations are not performed and controlled. ☻Inventory movements (for example whenever raw materials, outside services, and production suppliers are purchased, direct labor is incurred, production overhead is incurred, production activities have taken place and goods sold) are not accurately recorded in the system or lack actual movement and authorization. ☻Provisions for obsolete, damaged or lost inventory are not captured, input, recorded, and processed in the correct accounting period. ☻All details and amounts related to inventory costs are not included in the financial statements and disclosures. ☻Amounts reported in multiple places related to inventory are inconsistent, or computations and footings are incorrect. ☻Another important issue is with incorrect recording of purchase and production variances between actual costs and standard costs, and direct and indirect costs.

Actual Internal Control Tools and Practices:

- Invoice matched with PO-order and received quantity in SAP and the material number has a reference to the PO-number in the inventory master file
- SOD matrix excel file applies
- ERP-system and owned databases for different calculations which describe the controls in place
- Bill of Material is connected to the customer order and run through the Material Requisition Planning in the SAP information system for automating inventory movements
- A yearly re-calculation is performed for all products by reviewing underlying documents and minutes of meetings for budget

Table 14: Internal Controls on IT

INFORMATION TECHNOLOGY
Data Center Operational Controls:
☻IS / IT systems and services must be consistently available as required for financial reporting (inception, recording, processing and reporting of transactions). ☻Appropriate technical support must be available in case of downtimes and other system disruptions. ☻Special resources must be available and / or must be on standby during the period end financial closings and reporting of information. ☻Third party service providers and outsourced IS / IT services must be managed to satisfy IS / IT requirements related to financial accounting and reporting. ☻Recovery procedures and testing must be in place to ensure minimum disruption to business.
System Software Controls:
☻All acquisitions of and changes to system software, databases management, telecommunication software, security software, utilities and hardware must be properly reviewed and approved.
Access Controls:
☻Information security must be managed to guide consistent implementation of security policies. ☻An effective control process must be in place to periodically review the appropriateness of access rights in order to reduce the risk of unauthorized/inappropriate access to the organizations in relation to financial applications and data. ☻Procedures must be in place to add, modify, and delete user accounts in a timely manner resulting in current records at any time reflecting the actual access rights. ☻Information must be protected against alteration, and unauthorized interception, while contained in an application or in transit through the network. ☻IS / IT equipment (including PCs and mobile devices) and people must be protected against manmade and natural hazards.
Application System Development and Maintenance Controls:
☻All installations or changes, including emergency changes, to application software providing financial reporting functionality must be made in a controlled manner to ensure the solution fits the intended purpose without major problems. ☻When new systems (application and associated infrastructure) must be implemented or modified; controls must be added, modified, or redesigned so that applicable control objectives (of the impacted financial processes) must be achieved.
Entity-level IT / IS Controls:
☻The IS / IT architecture (hardware, software and infrastructure) must be defined and documented. ☻Applications must be documented in Application Register. ☻The IS / IT organization must be properly defined to support the IS / IT service needs for financial reporting to ensure compliance with legal, regulatory and contractual

obligations. ☻IS / IT users must be provided adequate knowledge and training for them to use application systems. ☻Changes to system and infrastructure must be available and introduced to the users to ensure trouble free operations. ☻Segregation of duties must be achieved within the IS / IT organization.
Actual Internal Controls Tools:
• Documentation on kinds of application used for financial reporting IS/IT organization chart and level of authorizations • Password protection on every workstation • IS/IT process flow and control documentation is updated • SAP R/3 ERP application supports the following processes: Financial accounting & reporting, Purchasing & accounts payable, and Projects • In-house applications include assurance, risk review, credit information, securitization, capital investment, and employment database

Table 15: Internal Controls on Payroll

PAYROLL
Control Objectives- Payroll Administration:
☻Payroll master file must be secured and accurately updated on a timely basis with new and approved information. ☻Payroll input data such as time and attendance must be accurate, complete and authorized prior to system input. ☻Special payroll transactions such as withholdings, other deductions or special payments must be authorized through the appropriate authority and documented. ☻Payroll payments must be made on a timely basis to the correct employees entitled to receive the payments. ☻Payroll payments and deductions must be accurately recorded as to the correct amount, account allocation and in the appropriate period. ☻Segregation of duties must be maintained in all related functions. ☻The review and authorization of the design of bonus schemes must be independent of those who will benefit from them. ☻Bonuses due to each employee under the scheme must be authorized and accurately calculated, recorded, deducted and paid. ☻If applicable, there must be on-going monitoring that appropriate internal controls policies and procedures exist at third party service providers to which payroll administration has been outsourced.
Control Objectives- Employee Business Expenses:
☻All expenses claims comply with policy must be approved and accurately calculated and payments must be made on a timely basis to the correct employees. ☻Accounting for business expense payments and transactions must be accurately classified, reconciled, coded and posted to the appropriate general ledger account.
Control Objectives- Pension & Post-Employment Employee Benefits:
☻Post-employment and post-retirement benefits comply with laws and regulations. ☻Affiliation to an employee benefit program must be authorized and approved. ☻All

changes to employee benefit schemes, plan amendments, curtailments and settlements must be authorized, approved and communicated within the entity. ☻All transactions related to post-employment and post-retirement benefits must be valid and related amounts must be calculated correctly. ☻Disclosure information related to post-retirement and post-employment benefits must be reported accurately. ☻If applicable, there must be on-going monitoring that appropriate internal controls policies and procedures exist at third party service providers to which employee benefits related activities have been outsourced.

Table 16: Internal Controls on Property, Plant & Equipment

PROPERTY, PLANT AND EQUIPMENT
Control Objectives:
☻Property, plant and equipments must have accurate values in accounting records with adequate financial statements disclosures and based on A&RG in appropriate accounting period. ☻Fixed asset general ledger control accounts must accurately reflect the assets recorded in the fixed asset register / sub ledger. ☻The property must be safeguarded and SoD must be achieved. ☻All assets disposal which are scrapped or retired must be accurately valued and not recorded. ☻Financial statement disclosures must include all details and amounts relating to plants, property and equipment in accordance with A&RG. ☻Periodic depreciation charges must be accurately recorded and calculated within appropriate period and A&RG. ☻All construction projects that satisfy the criteria of fixed assets must be accurately recorded. ☻Applicable interest on capitalization of assets for repairs and maintenance must be according to A&RG and made on-time. ☻Capital expenditures for acquisition must be approved and recorded accurately before being capitalized. ☻Asset financing through leasing must be decided / approved by authorized personnel and the decision must be based on sound and documented analysis. ☻Leased assets must be managed in compliance with lease agreements and recorded accurately on-time.

Table 17: Internal Controls on Projects

PROJECTS
Control Objectives:
☻Pertinent customer contract data must be accurately maintained on file and be physically secured. ☻Orders / contracts (including amendments and change orders) must be approved by management as to prices and terms of sale and recorded accurately. ☻Bidding and estimation of total project costs must be accurate and reliable and include all relevant cost components. ☻Project / contract terms must be reviewed prior to authorization and execution. ☻Project costs and provisions related to projects must be accurately valued and recorded. ☻Segregation of duties is

achieved. ☻Revenue recognition related to projects is in compliance with the A&RG. ☻Cost and progress information serving as input to the percentage of completion revenue and profit calculation is compiled accurately, completely and timely. ☻Estimates of the percentage of completion must be accurate and supported by the project status. ☻Billings in excess of sales and sales in excess of invoicing must be valued and classified in accordance with the A&RG. ☻Disputes and claims must be properly recorded. ☻Cash receipts must be properly processed when received.

Table 18: Internal Controls on Purchasing

PURCHASING
Control Objectives:
☻Approved vendor listing / master files must be accurately maintained. ☻Purchase orders must be created for legitimate needs and recorded accurately, identifying suppliers, quantities ordered, quality confirmed, prices and freight terms. ☻Firm purchase commitments are in accordance with the A&RG.
Financial Reporting Risks:
☻Vendor selection and changes to the master vendor file are made without proper authorization or actual vendor data. ☻All changes to the master vendor file are not captured, input, recorded, and processed into the information system in the correct accounting period. ☻All related parties are not accurately identified and captured in the vendor master file. ☻Purchase orders / agreements are raised without a legitimate purchase requisition. ☻Duplicate postings of purchase orders / agreements occur in the purchases subsidiary ledger or purchases are recorded in the wrong account due to incorrect coding. ☻Purchase requisitioning, authorization and recording functions are not segregated.
Actual Internal Control Tools and Practices:
• SAP master vendor file adds new vendors and banking information is supplied by another system • SAP can automatically check for input fields such as VAT code and automates several others • SAP access rights are reviewed and approved on the basis of log lists • Functions such as purchase order depend on purchase requisition as these are sequentially numbered by SAP to avoid duplication later • SOD is controlled by SAP-system profiles based on IT management

Table 19: Internal Controls on Revenues and Accounts Receivables

REVENUE AND ACCOUNTS RECEIVABLE
Control Objectives - Customer Orders:
☻Pertinent customer data must be accurately maintained on file. ☻Customer orders

must be only processed within approved customer credit limits. ☻Customer contracts / agreements must be physically secured and only valid customer orders must be input and processed. ☻Orders must be approved by management as to prices and terms of sale. ☻Orders and cancellations of orders must be input accurately, completely and timely. ☻Order entry data must be transferred accurately and completely to the manufacturing, shipping and invoicing activities. ☻Information related to customer orders must be communicated to the financial accounting and reporting process accurately, completely and timely in compliance with related A&RG requirements.
Control Objectives - Shipping and Invoicing:
☻All goods shipped or services rendered must be invoiced, and all invoices raised relate to authorized goods shipped or services rendered with exceptions also properly supported and approved. ☻Invoices must be accurately calculated and recorded accurately and timely. ☻Credit notes for all goods returned and adjustments to Accounts Receivable (AR) must be valid and accurately calculated. ☻Customer volume or other rebates must be accounted for accurately and in the correct accounting period, in compliance with the A&RG.
Control Objectives - Revenue Recognition:
☻Sales revenues and income must be recorded in the appropriate period. ☻Revenue arrangements with multiple deliverables must be accurately accounted.
Control Objectives - Accounts Payable:
☻Accounts receivable represent valid claims against customers and others, and balances must be accurately maintained and accurately valued. ☻SoD must be achieved.

Table 20: Internal Controls on Shareholders Equity

Shareholders Equity
Control Objectives:
☻Shareholders' equity transactions, such as cash disbursements or dividend payments, and Shareholders' equity balances must be authorized and accurately recorded within right accounting period in accordance with the A&RG and have adequate supporting evidence. ☻Stock certificates and original documents related to equity transactions must be safeguarded. ☻Statutory shareholders' equity must be reconciled to A&RG equity accurately and timely. ☻Items of other comprehensive income or loss must be accurately recorded and classified within shareholders' equity.

This closes the tabular depiction of internal control processes of company X.

For readers, who inquire about the absence of all financial reporting risks and internal control tools and practices, please refer to Methodology chapter for explanation of the redundancies involved and sampling rules. The definition of errors in chapter three will summarize nature of financial reporting risks for company X data.

Summary:

In this chapter, the thesis tried to provide answers to the problem statements from document observation, constant comparison method, and general contrast. The chapter started with answering the fourth problem statement that targeted finding the most efficient technology solution that can deter fraud with agility. The next attempt was to answer the functionalities of kinds of software, where each kind of software's key features. Lastly, descriptions of internal control processes of company X were in tables to describe key issues. The next section tries to conduct analysis on these results to rebuild theoretical details that must focus on IT, professional roles, and financial frauds.

Chapter Five

❖ ***Results Analysis***

This chapter analyzes the content from the previous chapters, by trying to build a correlation between IT, frauds, and professionals. In an attempt to secure the information for empirical results, documents on IT and professional roles did not gather importance previously. It became important to review such key IT features and base the analysis on combined sets of ideas. This section intends to measure relations between corporate governance and IT. It is important to review key elements of Fraud Deterrence Cycle that participate with IT, such as Segregation of Duties (SoD) and security authorizations. The analysis builds after testing the hypothesis in the previous chapter that logically recommended transaction and ERP systems as best suitable choice for antifraud tactics, because support in deterring fraud is available instantly to nonspecialist employees, even if professionals such as auditors may be vigilant into matters of frauds with their generic software tools.

1) Financial Experts and Software Use

Forensic Accounting investigators, forensic accountants and technologists, and auditors often use data mining software for testing accuracy. Since investigators arrive after possible surfacing of fraud, data mining, and audit-trails are key features expected from good software that detects frauds for forensic examination. Auditors equally use compliance and process management software with fraud detection tools. Internal auditors have more access to enterprise computer systems, and efficient use of business intelligence and transaction systems needs skilled auditors to understand the data mining with audit trails. However, at the end it is the duty of the management to implement all kinds of internal control reporting software tools and uphold acceptable clarity in business.

2) IT Governance

Simonsson and Ekstedt (2007) defined "IT governance as the preparation for, making of and implementation of IT-related decisions on goals, processes, people, and technology on a tactical or strategic level. Two different studies tried to explore the gap between IT governance priorities of IT governance experts and literature. Their results show the greatest differences are within the priorities of the decision-making phases. The literature highlighted the importance of monitoring decision-making at all-time, while practitioners claim that understanding and providing good contribution for decision-making is higher on their agenda."

a) SOX

Kaarst-Brown & Kelly (2005) listed SOX sections and their impact on CIO and IT functions. Two of the sections specifically target frauds and crime. Section IX for 'White-Collar Crime Penalty Enhancements' announces penalties for tries and conspiracies to commit fraud. It covers mail and wire fraud, employee retirement fund, corporate responsibility for financial reporting, and amendments to sentencing of white-collar offenses. To ensure compliance, IT must have organization in place to record and track any changes to the original information collected. All changes will need to be traceable, including information on anyone who made changes. Section XI for 'Corporate Fraud and Accountability' covers tampering a record or impeding an investigation. It enables temporary freeze authority for the SEC to restrict individuals from servings as officers or directors and ensures consequences for retaliation against informants. This section had an impact on data management because it increased involvement of IT to provide timely archival documents and summary data with expansion to Enterprise-wide risk management. Several models can guide CIO's and the IT work in their goal to support Sarbanes-Oxley compliance. Two of the existing frameworks that may aid with the issues are COSO and 'Control Objectives for Information and related Technology' (COBIT). COBIT (developed by the IT Governance Institute as part of the 'Information Systems Audit and Control Association' (ISACA)) is also an accepted standard that provides a guides for users, audits, control procedures, and security practices.

b) SOD

Segregation of duties (SoD) is important for internal controls. The reporting firm should have a clear outline on SoD in the documentation of the process descriptions. For this purpose, use of organization charts and responsibility/authority allocation is common. Within the process descriptions, functions should be specific enough to point to a particular person and be able to make an assessment about achieving SoD. For example, purchasing personnel, as a role is too general, since within purchasing there are various functions that should have separate roles that is, people approving suppliers, people entering suppliers into for example SAP. Regardless of the documentation format used, management must ensure the reader gets a clear view of the transaction flow in each class of transaction in the organization, from beginning of a transaction to final reporting in financial statements. A documented walkthrough of the different steps or activities in the process can accomplish SoD.

3) Information Technology and the CFO

CFOs are at the compliance sharp end because they are best qualified to understand the processes that underpin auditable systems. CFOs have an instinctive appreciation of document life cycle management from acquisition through to actions, onto referencing and finally disposition. Every organization generates communications, and most will have a value. Anything that has a value is of interest to CFOs, but compliance has a cost. The problem is how to make compliance a value enabler.

Overall, corporate responsibility for data quality has shifted more and more to the CFO whose role as champion for corporate compliance and control standards has always relied on the integrity of data in underlying systems. Corporate reporting relies on data quality depending on underlying systems such as ERP for manufacturing, Customer Resource Management

(CRM) systems for sales and marketing, financial systems for finance, and Human Capital systems for human resources. Poor data entry standards result in duplicate records that can cause confusion. Important issues with data include current data, migration, consolidation, data integration, replication, and synchronization. Data corruption can happen in many ways, which is a risk.

4) Information Technology versus Audit Committee

Spira's (1999) paper has explained, "The audit committee literature provides little clarity about the purpose of audit committees and, as a consequence, discussion of their effectiveness has limits and may be inconclusive. The assumptions underlying the Cadbury Code – that audit committees will protect auditor independence and thus lead to improved financial reporting – have been challenged and the study reported here indicates that audit committee participants are skeptical about the ability of audit committees to improve financial reporting quality by detecting fraud."

Nevertheless, the audit committee has foresightedness to develop new audit plans. Rezaee et al. (2002) recommended in an article "audit committees must strongly support real-time financial reporting so investors can access corporate information in shorter periods. The real-time reporting outline is a possibility in next ten years. Considering compliance issues were unheard-of couple of years back, and that internet is developing its own suite of software solutions, integration of real-time reporting into continuous monitoring solutions is an important issue."

5) Information Technology and the Auditors

Lynn Edelson, partner and U.S. leader for systems and process assurance at PricewaterhouseCoopers commented, "Senior IT management needs to start talking with the external auditors about IT controls, including documentation and testing, quarterly reviews of significant changes in the IT environment, audit committee IT oversight and fraud controls." Information and IT must be protected against harm from vulnerabilities such as loss, inaccessibility, change, and wrongful disclosure, whether they are caused by errors and omissions, fraud, accidents, or intentional damage (Damianides 2007).

By adopting a transactional analysis model for continuous monitoring and auditing of controls, auditors can assess controls effectiveness based on the evidence of the transactions. One can achieve extra assurance by directly testing certain types of IT system controls within the continuous monitoring process. Such controls are usually in accordance to an information systems controls framework such as the IT Governance Institute's CoBIT. These controls include, for example, systems access and authorization rights to ensure effective segregation of duties, as well as configuration settings within an ERP system.

On the contrary, Debreceny et al. (2006) conducted a software research on the banking industry, and the results were similar to company X because most banks also use in-house software extensively. “Computer assisted audit techniques (CAATs) encompass computerized techniques that internal and external auditors use to ease their audit objectives. One of the most important CAATs is generalized audit software (GAS), which is a class of packaged software that allows auditors to interrogate various databases, application software and other sources and then conduct analyzes and audit routines on the extracted or live data. The research found the extent and range of use of GAS varies widely between the institutions in the sample. Internal auditors see GAS primarily as a tool for special investigations rather than as a foundation for their regular audit work. External auditors make no use of GAS, citing the inapplicability of this class of tool to the nature of testing the financial statement assertions or the extent or quality of computerized internal controls maintained by the bank. The common uses of GAS include extraction of samples, identification of reactivated dormant accounts and verification of the completeness and accuracy of data. This study also found that GAS is often in use for special investigation audits. From these findings, it becomes clear that bank auditors do use GAS, but only to a limited extent. Findings of this study provide some possible reasons for the limited use of GAS. One common reason is that some banks have their own in-house customized banking systems whose capabilities are similar or even superior to those of GAS. GAS is usually not considered a routine substantive testing procedure. The study also finds that auditors are often more concerned about testing compliance and internal controls effectiveness than performing substantive testing. There is also evidence that difficulty in using GAS and the question of cost-effectiveness hindered its use. The study found that external auditors from the major professional accounting firms make no use of GAS, either in the conduct of the IS component of the external audit or in testing financial statement assertions. One finding on lesser use of GAS by bank internal auditors is that they perceive GAS as interrogation tools to perform fraud investigations rather than as general audit tools."

6) Contrasting IT with Accountant's Role

After considering accountants in the company and external public accounting firms as likely candidates for the job of advising companies on compliance with the Sarbanes Oxley act (SOA), Schneider & Bruton (2004) found them "lacking in technical expertise, independence, and overall business knowledge. Therefore, IT professionals have higher degrees of relevant technical expertise and sufficient levels of overall business knowledge for qualifying to advise companies on SOA compliance efforts, especially if their technical knowledge increases by legal training. This legal training is more relevant to some areas of SOA compliance than the others. IT professionals have a strong advantage over the accounting industry in this comparison: IT professionals have no stigma by an association with frauds, irregularities, and crimes that motivated the SOA's passage. Accountants in general and public accounting firms in particular, cannot make that claim."

Summary

This chapter tried to analyze IT development with the involvement from key professionals in Accounting and Finance. The roles of CIO and the IT department also hold key position when setting up computer systems that can deter fraud. The chapter tries to present the dependency on IT by financial experts and builds on a conviction that software can automate fraud deterrence to the maximum-level during monetary-based transactions. It provides expanded view of the theoretical data by associating members of corporate governance with IT role for deterring fraud.

Chapter Six

❖ Conclusion of the Thesis

While prevention of financial frauds would be a desirable outcome for corporate governance programs, complete prevention is impossible. Deterrence, therefore, offers a more sensible view. Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2 focuses on transaction-level controls, which are accounting and financial controls designed to ensure that only valid, authorized, and legitimate transactions occur and to safeguard corporate assets from loss because of theft or other fraudulent transactions. These procedures are preventive because they may actively block or prevent a fraudulent transaction from occurring. Anti-money laundering procedures employed by financial institutions are an excellent example of a processes designed to deter fraudulent transactions. Corporate Governance and transaction-level controls are the first lines of defense against fraud and deter fraud by occurring on the first place. This chapter will explain the answers to the problem statements in simple layout. Later, a brief paragraph will suggest future suggestions related to this study.

Findings of the Study

On the overall, the focus of the thesis was to answer the question: ""How may various IT-solutions help different professionals in detection and correction of financial frauds?" On a theoretical front, the question implied understanding individual units of transaction-level controls and corporate governance. The theoretical guide provided an excellent platform to resolve the interdependencies in professional roles and financial fraud deterrence. It answered the first subquestion and laid a foundation of where to expect preventive actions against frauds.

The second subquestion’s focus was to provide an insight into business processes of SOX section 404. The study needed to find authentic information to summarize range of business processes that might define control objectives, with basic corporate ideology on financial reporting risks in a particular process. The documents were originally from the company X intranet that was accessible only after paying several visits to the firm. Later, the documents provided a listing of business processes, which was grouped to assist in comparing different software offerings. SAP became a choice as company X depends on it mostly. The research finding suggested that several financial reporting risks tend to sound similar to others and generalization of recurring risks is necessary. In addition, findings stated that even though company X was not using most kinds of software, several of its actual internal reporting controls depended on document management and workflows, with efficient collaboration in Lotus Notes and transaction processing through SAP, which provides real-time integration of data within the company network because it is an ERP system.

The third subquestion required broad comparison of some of the existing specialized software kinds. The question was peculiar since it implied broad classification of a few vendor firms, where grouping of special features of chosen vendor software were useful in cross-comparisons later. But, the section was useful in giving contrast of each kind of software, and later with the vendor firms within each kind. One of the finding was that audit-trails were common to all software, with focus on detection of fraud at various transaction levels. However, the focus of the thesis was on fraud deterrence, therefore software that reduced chances of fraud were the most interesting for the thesis objectives.

Answering the fourth subquestion was possible after coding, grouping, and examining field notes. A major finding was that fraud deterrence in transaction-level controls is best possible with transaction-systems and continuous-controls-monitoring IT solutions. In most cases, high-speed internet can bolster the possibilities of monitoring data in real-time without long delays. Hence, the suggestion from the research findings was that any software was inadequate for implementing fraud deterrence, only because of disjoint computer software for various steps involved in internal control reporting. In contrast, combination of software features could provide substantial fraud deterrence, like ACL.

Suggestions for the future

In the future, continuous control systems will advance into more diversified solutions, which may be available on the internet. The research field is technical, but it is of constant interest to financial professionals. Furthermore, interview based study on types of business software can provide primary data based research. The interviews must speculate on the range of software integration that is necessary to deter financial frauds among the various kind of software used for internal control reporting. Surveys can inquire about efficiencies in software for monitoring controls from different firms.

Appendix

This section contains figures for illustrative purposes only.

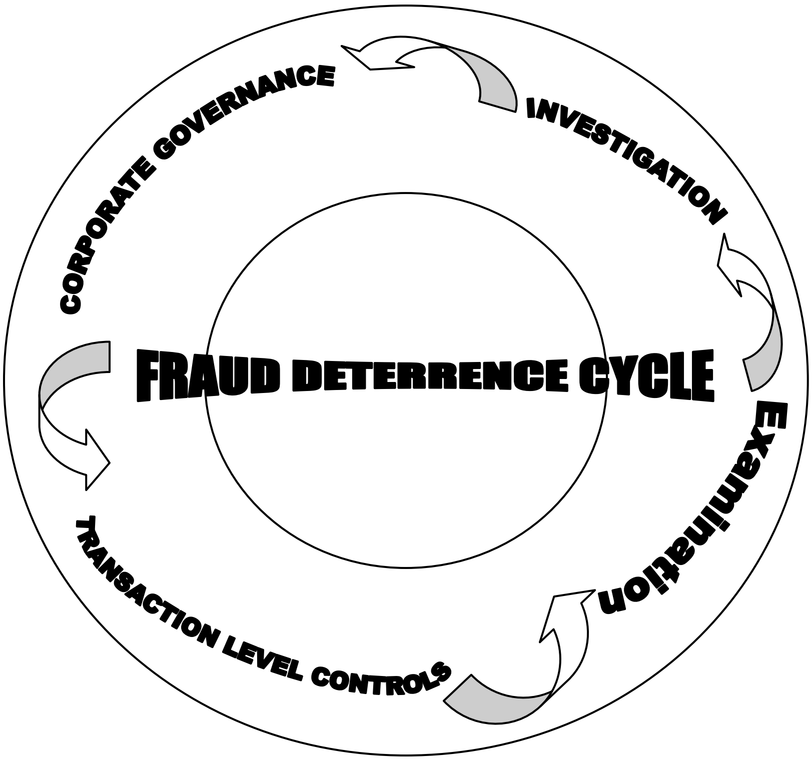

Figure 1: Fraud Deterrence Cycle

Adapted from Skalak, S., Alas, M. & Sellitto, G. 2004, 'Fraud: An Introduction', in *A Guide to Forensic Accounting Investigation*.

Ideally, this picture must accompany the first chapter where most of the details can be found for FRAUD DETERRENCE CYCLE. It is important to understand that deterrence implies slowing the process of fraud. It is different in meaning from prevention and detection.

Type of Fraud	*Tests Used to Discover This Fraud*
Fictitious vendors	Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers
	Be alert for vendors with similar sounding names or more than one vendor with the same address and phone number
Altered invoices	Search for duplicates
	Check for invoice amounts not matching contracts or purchase order amounts
Fixed bidding	Summarize contract amount by vendor and compare vendor summaries for several years to determine if a single vendor is winning most bids
	Calculate days between close for bids and contract submission date by vendor to see if the last bidder consistently wins the contract
Goods not received	Search for purchase quantities that do not agree with contract quantities
	Check if inventory levels are changing appropriate to supposed delivery of goods
Duplicate invoices	Review for duplicate invoice numbers, duplicate date, and invoice amounts
Inflated prices	Compare prices across vendors to see if prices from a particular vendor are unreasonably high
Excess quantities purchased	Review for unexplained increases in inventory Determine if purchase quantities of raw materials are appropriate for production level
	Check to see if increases in quantities ordered compare similarly to previous contracts or years or when compared to other plants
Duplicate payments	Search for identical invoice numbers and payments amounts
	Check for repeated requests for refunds for invoices paid twice
Carbon copies	Search for duplicates within all company checks cashed; conduct a second search for gaps in check numbers
Duplicate serial numbers	Determine if high value equipment a company already owns is being repurchased by checking serial numbers for duplicates and involvement of same personnel in purchasing and shipping processes
Payroll fraud	Find out if a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck and extract all pay transactions for departure date less than date of current pay period
Accounts payable	Reveal transactions not matching contract amounts by linking Accounts Payable files to contract and inventory files and examining contract date, price, ordered quantity, inventory receipt quantity, invoice quantity, and payment amount by contract

Figure 2; Types of Frauds and Computer Tests

Adapted from Coderre, D. G. 1999, Fraud Detection, Using Data Analysis to Detect Fraud, Global Audit Publications, Vancouver.

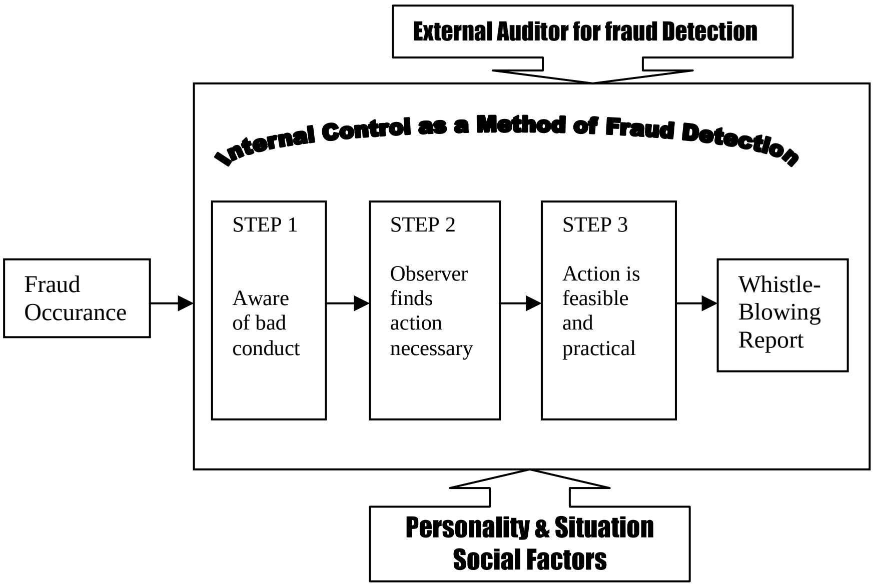
External Auditor for fraud Detection
Internal Control as a Method of Fraud Detection
Fraud Occurance
STEP 1
Aware of bad conduct
STEP 2
Observer finds action necessary
STEP 3
Action is feasible and practical
Whistle-Blowing Report
Personality & Situation Social Factors

Figure 3: Whistle-Blowing Process Model

Adapted from Miceli, M. P. & Near, J. P. 1992, *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees*, Lexington Books, New York.

Reference List

ACL. 2007, Available from: <www.acl.com>.

AICPA. 1988, *Statement on Auditing Standards (SAS) No. 61 - Communication with Audit Committees*, AICPA, New York.

AICPA. 1997, *Consideration of Fraud in a Financial Statement Audit - SAS No. 82*, AICPA, New York.

AICPA. 1999, *Statement on Auditing Standards (SAS) No. 89 - Audit Adjustments*, AICPA, New York.

AICPA. 2000, *Statement on Auditing Standards (SAS) No. 90 - Audit Committees Communications*, AICPA, New York.

Approva. 2007, Available from: <www.approva.net>.

Aronow, G., Karron, A. & Thomas, J. 2004, 'Auditor's Responsibilities and the Law', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 75-86.

Axentis Enterprise. 2007, Available from: <www.axentis.com>.

Beasley, M. S. 1998, 'Board of Directors and Fraud', *The CPA Journal*, pp. 56-58.

Beneish, M. D. 1999, 'The Detection of Earnings Manipulation', *Financial Analysis Journal*, vol. 55, no. 5, pp. 24-36.

Best, P. (2005/11/04), *Project Frodo Progress Report*, [Online], Available from: <http://www.isi.qut.edu.au/research/publications/technical/qut-isi-tr-2005-012.doc>.

Bishop, T. S. F. 2007, *Fraud Detection and Prevention Tips for Audit Committee*, [Online], Available from: <http://AMRWD5953.arthurandersen.com/website.nsf/content/MarketOfferingsAssuranceResourcesFraudPrevention>.

Blue Ribbon Committee (BRC). 1999, *Report and Recommendations of the BRC on Improving the Effectiveness of Corporate Audit Committees*, NYSE and NASD.

Bruton, C. M. & Schneider, G. P. 2004, *Information Technology Professionals or Accountants: The Best Choice for Sarbanes-Oxley Compliance*, [Online], Available from: <http://www.sbaer.uca.edu/research/allied/2004/academySciences/pdf/14.pdf> [18 Dec 2006].

BusinessObjects. 2007, Available from: <www.businessobjects.com>.

Caseware's IDEA. 2007, Available from: <http://www.horwath.com.au/services/software/software_idea.asp>.

Certus. 2007, Available from: <www.certus.com>.

Coderre, D. G. 1999, Fraud Detection, Using Data Analysis to Detect Fraud, Global Audit Publications, Vancouver.

Cognos. 2007, Available from: <www.cognos.com>.

Corbett, M. & Clayton, M. 2004, 'Analyzing Financial Statements', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 365-383.

Counterstrike. 2007, Available from: <www.counterstrike.com/frauddet.html>.

Damianides, M. 2007, *Sarbanes-Oxley And IT Governance: New Guidance On IT Control And Compliance*, [Online], Available from: <http://www.infosectoday.com/SOX/Damianides.pdf> [18 Dec 2006].

DeAngelo, L. 1986, 'Accounting Numbers as Market Valuation Substitutes: A Study of Management Buyouts of Public Stockholders', *The Accounting Review*, vol. 61, pp. 400-420.

Debreceny, R., Lee, S.-L., Neo, W. & Toh, J. (2006/05/10), *Employing generalized audit software in the financial services sector - Challenges and opportunities*, [Online], Available from: <http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=Published/EmeraldFullTextArticle/Pdf/0510200604.pdf> [19 Dec 2006].

DeChow, P. M., Sloan, R. G. & Sweeney, A. P. 1996, 'Causes and Consequences of Earnings Manipulation: An Analysis of Firms Subject to Enforcement Actions by the SEC', *Contemporary Accounting Research*, pp. 87-103.

Dooley, D. & Skalak, S. 2004, 'Financial Reporting Fraud and the Capital Markets', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 59-73.

eFileCabinet. 2007, Available from: <www.efilecabinet.com>.

EMC. 2007, Available from: <www.emc.com>.

Extensity. 2007, Available from: <www.extensity.com>.

FileNet. 2007, Available from: <www.filenet.com>.

Gerson, J., Brolly, J. & Skalak, S. 2004, 'The Roles of the Auditor and the Forensic Accounting Investigator', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 21-46.

GoFileRoom. 2007, Available from: <www.immediatech.com>.

Golden, T. W., Dyer, M. & Andreassen, S. 2004, 'Working with Attorneys', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 475-492.

Graham, J. W. 1986, *Principled Organizational Dissent: A Theoretical Essay in Research in Organizational Behavior*, JAI Press, Greenwich.

Handysoft BizFlow. 2007, Available from: <www.handysoft.com>.

Holmes, S. A., Langford, M., Welch, O. J. & Welch, S. T. 2000, *An investigation of the relationships between organizational citizenship and the characteristics of fraud - Working Paper*, Texas A&M University.

Hooks, K., Kaplan, S. & Chultz, J. S., Jr. 1994, 'Enhancing Communication to Assist in Fraud Prevention and Detection', *Auditing: A Journal of Practice and Theory*, pp. 86-117.

Hyperion. 2007, Available from: <www.hyperion.com>.

International Business Machines. 2007, Available from: <www.ibm.com>.

Kaarst-Brown, M. & Kelly, S. 2005, *IT Governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function?*, [Online], Available from: <http://csdl2.computer.org/comp/proceedings/hicss/2005/2268/08/22680236a.pdf> [Dec 18 2006].

Kenyon, W. & Tilton, P. D. 2004, 'Potential Red Flags and Fraud Detection Techniques', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 119-160.

Metastorm. 2007, Available from: <www.metastorm.com>.

Miceli, M. P. & Near, J. P. 1992, *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees*, Lexington Books, New York.

Moulton, P. (2002/03/28), *Fraud Auditing within a SAP R-3 Environment*, [Online], Available from: <http://www.accountancy.com.pk/docs/Fraud_auditing_in_a_SAP_environment.pdf>.

Movaris. 2007, Available from: <www.movaris.com>.

Paisley. 2007, Available from: <www.paisleyconsulting.com>.

Pickett, K. H. S. & Pickett, J. 2002, *Financial Crime Investigation and Control*, John Wiley & Sons, New York.

Power, E. & Trope, R. , *Sailing in Dangerous Waters: A Director's Guide to Data Governance*, [Online], Available from: <http://books.google.com/books?hl=en&lr=&id=fDCNhdgI36sC&oi=fnd&pg=PA1&sig=iEHuQNxhWKfY-4pPxT5nZBYAyBE&dq=fraud+technology+software+system+corporate+governance&prev=http://scholar.google.com/scholar%3Fq%3Dfraud%2Btechnology%2Bsoftware%2Bsystem%2Bcorpo> [19 Dec 2006].

Public Oversight Board (POB). 2000, 'The Panel on Audit Effectiveness Report and Recommendations', POB, Stamford.

Ranallo, L. F. 2004, 'Forensic Investigations and Financial Audits: Compare and Contrast', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 109-117.

Rezaee et al. 2002, *Continuous Auditing: Building Automated Auditing Capability*, [Online], Available from <http://www.atypon-link.com/AAA/doi/pdfplus/10.2308/aud.2002.21.1.147> [2007-01-09].

Rezaee, Z. 2002, *Financial Statement Fraud - Prevention and Detection*, John Wiley & Sons, New York.

Seaman, C. 2007, *Qualitative Methods in Software Engineering Research*, [Online], Available from: <www.research.umbc.edu/~cseaman/> [06-12-17].

Simonsson, M. & Ekstedt, M. 2007, *Prioritizing IT Governance: Literature Vs Practice*, [Online], Available from: <http://www.ics.kth.se/Publikationer/Working%20Papers/EARP%20Working%20Paper%20Series%20MS105.pdf>.

Skalak, S. & Golden, T. W. 2004, 'Independence, Objectivity, Skepticism', in *A Guide to Forensic Accounting Investigation*, John Wiley & Sons, Hoboken, pp. 87-107.

Skalak, S., Alas, M. & Sellitto, G. 2004, 'Fraud: An Introduction', in *A Guide to Forensic Accounting Investigation*, pp. 1-20.

Spira, L. F. 1999, 'Ceremonies of Governance: Perspectives on the Role of the Audit Committee', *Journal of Management and Governance*, vol. 3, no. 12/12/06, pp. 231-260.

Stolowy, H. & Lebas, M. 2005, *Corporate Financial Reporting - A Global Perspective*, Thomson Learning, London.

Stone, P. (2005/10/31), *Anti-Fraud Programs and Controls: Combating Fraud and Misconduct Risk*, [Online], Available from: <http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/HotIssuesAnti-FraudProgramsandControls>.

Toronto Stock Exchange (TSE). 1994, *Where Were the Directors? Guidelines for Improved Corporate Governance in Canada*, The Dey Report.

Winters, B. 2004, *Choose the Right Tools for Internal Control Reporting*, [Online], Available from: <www.aicpa.org/pubs/jofa/feb2004/winters.htm> [22 Dec 2006].