RESTORING TRUST BY VERIFYING INFORMATION INTEGRITY THROUGH CONTINUOUS AUDITING

by

Stephen Flowerday

RESTORING TRUST BY VERIFYING INFORMATION INTEGRITY THROUGH CONTINUOUS AUDITING

by

Stephen V. Flowerday

Thesis

submitted in fulfilment of the requirements for the degree

Doctor Technologiae

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Promoter: **Prof. Rossouw von Solms**

December 2006

ABSTRACT

Corporate scandals such as Enron, WorldCom and Parmalat, have focused recent governance efforts in the domain of financial reporting due to fraudulent and/or erroneous accounting practices. In addition, the ineffectiveness of the current system of controls has been highlighted, including that some directors have been weak and ineffective monitors of managers. This board of director 'weakness' has called for additional mechanisms for monitoring and controlling of management, focusing on financial reporting. This problem intensifies in that today companies function in real-time, and decisions are based on available real-time financial information. However, the assurances provided by traditional auditing take place months after the transactions have occurred and therefore, a *trust problem* arises because information is not verified in real-time. Consequently, the errors and fraud concealed within the financial information is not discovered until months later.

To address this trust problem a conceptual causal model is proposed in this study based on the principles of systems theory. The emergent property of the causal model is *increased trust and control*. This study establishes that mutual assurances assist in building trust and that information security assists in safeguarding trust. Subsequently, in order to have a positive relationship between the company directors and various stakeholders, uncertainty needs to be contained, and the level of trust needs to surpass the perceived risks. The study concludes that assurances need to be provided in real-time to restore stakeholder confidence and trust in the domain of financial reporting. In order to provide assurances in real-time, continuous auditing is required to verify the integrity of financial information when it becomes available, and not months later. A continuous auditing process has its foundations grounded in information technology and attends to the challenges in real-time by addressing the *standardisation of data* to enable effective analysis, the validation of the *accuracy* of the data and the *reliability* of the system.

DECLARATION

I _____, hereby declare that:

- The work in this thesis is my own work.
- All sources used or referred to have been documented and recognised.
- This thesis has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

_____

ACKNOWLEDGEMENTS

Nothing significant is ever achieved alone. I am indebted to many individuals for their help and support. I would like to publicly express my gratitude to the following:

- For Jacqui, my eternal companion, for her love, sacrifice and care.
- For Ethan, Callum and Erin, for their enthusiasm and patience.
- For Mom and her constant encouragement.
- For Elsa Strydom, staff at the NMMU, whose support was invaluable.
- Finally for Rossouw von Solms, my promoter, who has become my mentor and friend and has made this experience what I hoped it would be.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

"Art and science have their meeting point in method."
- Edward Bulwer-Lytton, (poet, 1803-1873)

1.1 PROLOGUE

Lapses in good corporate governance as well as fraudulent and/or erroneous accounting practices have left the various company stakeholders, including investors, wary of the information found in company financial statements. The image of boards of directors and the auditing profession has been tarnished due to substandard financial reporting and outright fraud. For one to *trust* the information found in the various financial statements, assurances need to be provided that the integrity of the information has not been compromised.

This research project does not try to identify how to restore confidence in general in the boards of directors, rather it focuses specifically on the very important domain of financial reporting. It investigates what causes the lack of stakeholder trust, including diminished investor confidence. Relevant chosen topics, found to be contributing dimensions of the problem, have been investigated and a proposed solution is presented. These dimensions are covered in the various chapters and together with the proposed solution of continuous auditing, which provides assurance in real-time and on demand, help to restore stakeholder confidence.

Although the research is carried out within the specific area of interest described above, it is encompassed within the wider area of corporate governance and in particular, information security governance. During this study it was found that an understanding of the condition of the information, that makes up the financial statements, is required. An insight as to whether the information has integrity or not, is vital to the decisions based on that information. Without this insight, the inherent uncertainty involved in these decisions will be high.

In the 21st century, business is conducted in real-time with decisions based on real-time financial information. The current system of providing assurances is almost archaic in that the assurances are provided months after the transactions have occurred. Therefore, this research project proposes that assurances need to be provided in real-time so that stakeholder confidence can be restored.

Today it is accepted that IT systems are inextricably linked to the financial reporting processes (IT Control Objectives for Sarbanes-Oxley, 2004). Financial information is the main output of financial information systems, and information technology *'IT'* is the technology used to produce and manage this information. As early as 1949 (Shannon & Weaver), it was recognised that the technology or the technical level of a communication system must ensure the accuracy and efficiency of the information the system produces. In other words the *"noise"* in the system, as referred to by Shannon and Weaver (1949), should not corrupt or distort the information between the source and destination. Therefore, a trustworthy system requires that all technologies which form part of the system, should aim to protect and ensure the information's integrity.

As stressed, for real-time financial information systems, real-time assurances need to be provided (Alles, Kogan & Vasahelyi, 2005; Flowerday & Von Solms, 2005a; Onions, 2003). This research project emphasises internal controls as an integral part of enterprise risk management, which in turn is part of the broader management process (COSO-ERM, 2004). Furthermore, this is in agreement

with Boritz (2005) who contends that to ensure that the information has its integrity, one needs to *'control'* both the *data* and the *system*.

The directors and management have the responsibility to ensure that the integrity of the information embedded in the business processes, especially the financial processes that make up the financial statements, is untainted. This research project will emphasise a process as part of the solution - *The Continuous Auditing Process*. This process extends beyond the automation of existing auditing methods. This research project will address the issue of providing *assurance on demand* by verifying information integrity in real-time. These real-time assurances will assist in restoring stakeholder confidence and trust, within the domain of financial reporting.

1.2 DESCRIPTION OF PROBLEM AREA AND PROPOSED SOLUTION

This section highlights the need to address the integrity of information found within company financial statements. It proposes continuous auditing with its foundations grounded in information technology, as the method of restoring stakeholder confidence, by providing real-time assurances. This is to be done in addition to a system of internal controls and a monitoring system of these controls. Trust will then be restored when uncertainty is reduced and assurances are provided that the information's integrity is intact.

1.2.1 Breakdown in Financial Reporting

The recent fraudulent transactions and financial calamities created by Enron, WorldCom, Tyco, Parmalat, and the East Asia crises, have turned the spotlight on corporate governance and financial statements. As a result, the current financial reporting model is being heavily scrutinised and this is evident in the recent significant regulatory reform measures being considered and implemented. The consequence of these *breakdowns* has left the various

stakeholders wary and lacking faith in the integrity of published financial statements.

It is therefore essential that confidence and trust be re-instated in the boards of companies pertaining to their financial statements. To restore trust is not an easy task, considering that risk and trust appear to be significant variables. Risk needs to be managed adequately in order to safeguard trust. This indulges the assumption that to have confidence in information security requires trust, and trust requires information security to help safeguard it (a causal relationship which will be discussed in more detail in Chapter 9). Hence today in the management of risk, a system of internal controls is to be used to limit uncertainty. This will assist in providing assurances that the threats to the financial information systems are being adequately addressed.

1.2.2 Restoring Trust

Can there be any doubt that the corporate governance components of fairness, accountability, responsibility, and transparency (King II Report, 2002) contribute to the building and safeguarding of trust? Trust is not something that simply happens. It is fragile and not easily measured or identified (Handfield & Nichols, 2002). However, trust and controls are both needed to help curtail opportunistic behaviour, thereby achieving confidence in risk management. It has therefore become imperative that security for the financial information systems is comprehensive. Both opportunistic behaviour, which involves a human element, and the conventional technical IT security threats, need to be addressed.

Accordingly, it is stressed that, *"security is not a separable element of trust"* (Camp, 2002, p.27). This statement collaborates that both trust and security-based mechanisms are classified as safeguarding protective measures (Ratnasingham & Kumar, 2002). Together these provide technological, organisational and relationship benefits to the various company stakeholders. To have confidence, trust needs to increase and uncertainty needs to be reduced to

an acceptable level. This can be achieved through assurances given by auditors (ability), or through evolving relationships (discussed in game theory) where integrity and benevolence are considered. To avoid unfavourable behaviour, uncertainty needs to be contained and the level of trust needs to surpass the perceived risks. This will ensure that a relationship will flourish. It is therefore important to note that many of the elements that reduce risk are the same elements that increase trust (Gefen, Rao & Tractinsky, 2002).

This research project examines the concept of trust and uncertainty reduction followed by what constitutes trustworthiness. Self-centred opportunism, 'cheating' and dishonesty are classified as unfavourable behaviour. Behaviour is addressed using game theory to illustrate possible outcomes. The very close relationship between trust and risk, is discussed with assurances being emphasised as an element to help build trust. Finally, a trust strategy is recommended as a way to avoid unfavourable behaviour and to *build* and *safeguard* this concept of trust.

When one considers whether to place confidence in, and to trust the information found within the financial statements, three areas are to be considered. Firstly, information security which is concerned with the *reliability* of the information (confidentiality, integrity and availability). This leads to the assessment and identification of control deficiencies which highlight areas of potential risk, also referred to as control-based risk identification and management. Secondly, intentional or unintentional errors need to be eliminated. Fraud (intentional errors) is a concern when considering the *accuracy* of the information. Therefore, performing risk assessments (e.g. identification of exceptions preformed by analytical procedures) highlights processes or systems that experience higher than expected levels of risk. Thus, by examining risk one can identify areas where controls are inadequate (risk-based approach). It is therefore important that reliable information is accurate in the first instance. Thirdly, trust is concerned with *validity* (personal communication, Alex Todd, August 2005). Todd advocates that the auditor examines and assesses the

evidence that transactions are/were processed reliably and accurately, and thereby the auditor becomes a source of trust for the company.

1.2.3 Internal Controls

The safeguards, installed to ensure that the company's internal information is reliable and accurate, are referred to as internal controls. Companies have, as part of their risk management, a system of internal controls intended to counteract the inherent risks. Lindberg (2005) points out that internal controls can take the form of operational, financial, or administrative controls.

A reliable system of internal controls increases the probability that transactions are recorded correctly, therefore fraud and errors should not occur and the financial information should be reliable (Flowerday & Von Solms, 2005a). Important to note is that the establishment and maintenance of a system of internal controls are the responsibility of management (Braiotta, 2002; COSO-ICF, 1992; Horton, Le Grand, Murray, Ozier, & Parker, 2000; Hunton, Bryant, & Bagranoff, 2004). Furthermore, internal auditors should make recommendations to management for improvements to the controls or procedures, but they are not responsible for the system of internal controls.

Additionally, specific IT controls support governance and business management as well as provide general and technical controls over policies, processes, systems and people that comprise IT infrastructures (GTAG1, 2005). These include the processes that provide assurances for information and assist in managing the associated risks.

1.2.4 A Continuous Auditing Business Process

Today, orderly processes are necessary to provide an effective audit trail for the flow of data. Such processes are critical if auditors are to adequately assess strengths and weaknesses in the information security and internal control environments as well as audit transactions in real-time (Warren & Parker, 2003).

The influential American Sarbanes-Oxley Act of 2002, specifically Section 409, has created an increased demand for continuous auditing and the internal auditor plays a key role in this process (Daigle & Lampe, 2003). Additionally, real-time financial reporting is likely to necessitate continuous auditing. One would need to provide continuous assurances about the quality and credibility of the information presented (Rezaee, Shabatoghlie, Elam & McMickle, 2002). Continuous auditing is defined by Rezaee et al. (2002, p.147) as *"a comprehensive electronic audit process that enables auditors to provide some degree of assurance on continuous information simultaneously with, or shortly after, the disclosure of the information"*.

It is claimed by Flowerday and Von Solms (2005b) that continuous auditing can systematically and continually test transactions using intelligent software tools in real-time. They continue to emphasise that the auditor prescribes the criterion and the process identifies anomalies or exceptions, for which additional audit procedures should then be performed. Depending on the findings, the auditor may issue a report.

The growth of ERP (Enterprise Resource Planning) systems, increased bandwidth and use of the Internet, the speed of processing and the globalisation of business, have all contributed to the development of more intelligent software tools (Rezaee et al., 2002; Vasarhelyi, Alles & Kogan, 2003). These developments provide management and auditors with the ability to better capture and analyse key data for decisions. The use of intelligent agents, embedded in audit modules to monitor and trigger alarms when unusual transactions or patterns occur, provides management with tools to better monitor business processes (Warren & Parker, 2003).

While the auditing profession has long discussed the concept of continuous auditing, it has remained chiefly in the academic domain (Onions, 2003; Rezaee et al., 2002; Warren & Parker, 2003). Nevertheless, this thesis provides sound practical suggestions as to *what* a continuous auditing system needs to

accomplish and *how* to implement this system. Moreover, there are strong drivers for this process and change in auditing methods. Marks (2001) identifies that companies are rapidly installing new technologies requiring auditors not only to understand them, but also to assess the risks associated with these technologies. As early as 1989 (Groomer & Murthy), it was recognised that information systems in companies were becoming increasingly complex and the traditional audit trail was disappearing. As a result, internal control and security have become critical concerns.

1.3 PROBLEM STATEMENT

The result of the corporate scandals has been a loss in stakeholder, especially investor, confidence. Additionally the ineffectiveness of the current system of controls has been highlighted by these financial scandals. Consequently, this has led to a plethora of new regulations, guidelines, codes and standards, effective in stating *what* needs to be done rather than *how* it is to be done.

The problem is further exacerbated when one focuses on the monitoring and reporting of anomalies or exceptions, which companies are required to do. As stated within the Sarbanes-Oxley Act (2002), these weakness and deficiency disclosures as well as material changes need to be done on a *rapid and current* basis.

This problem intensifies in that today companies function in real-time and directors make decisions based on available real-time financial information. However, the assurances provided by auditors take place months after the transactions have occurred and therefore a *trust problem* has arisen because information is not verified in real-time. Therefore, the errors and fraud concealed within the information is not discovered until months later, after decisions have been made based on this information.

Thus, because assurances have not been provided in real-time, for real-time financial information, a trust problem has occurred. Company stakeholders have demonstrated a lack of trust in the directors as the financial statements have lacked integrity.

1.4 RESEARCH OBJECTIVES

The primary objective of this research is to produce a *causal model* that will result in increasing stakeholder confidence and trust in the domain of financial reporting. To achieve the primary objective, a number of secondary objectives should be addressed. These are:

- A study of the theories and processes underlying corporate governance and the causes of corporate financial scandals.
- An investigation into the various trust theories and the relationship trust has with uncertainty, risk and behaviour.
- Determining the role of the audit committee, the function of internal controls relating to financial statements and information security.
- Determining the elements of what constitutes information integrity and assurances specifically within the domain of financial statements.
- Identifying attributes of a company suggesting that a continuous auditing process is appropriate, including available technologies.
- Determining if the proposed continuous auditing models will assist in verifying financial information integrity in real-time and provide assurances on demand.

It is argued, in line with systems theory, that these secondary objectives (or parts of the problem) together form a *whole*. This is based on the concept that the *"whole is greater than the sum of its parts"* (Hanson, 1995, p.137). Hanson expounds and posits that the whole and the relationship between the parts becomes the focus of attention. Thus, causality becomes an issue as changing one part of the system changes all parts and affects the whole. Hence, a causal model is apposite for this research project.

1.5 RESEARCH DESIGN

According to Mouton (2001), the research design is tailored to address the research problem or question and there are various design types. This study does not involve empirical research, but it does involve philosophical and conceptual analysis, theory building and critical thinking.

1.5.1 Research Paradigm

Any piece of research will have an underlying philosophical paradigm, a pattern or shared way of thinking to which the research is aligned. A wide variety of philosophical paradigms exist, arising out of different ideas, views and perspectives of the world. This, in turn, leads to diverse ideas as well as the kinds of research questions and processes used to find solutions (Oates, 2006). This section discusses the research paradigm for this study. Figure 1.1 is used to illustrate these paradigms. Overall this research project is positioned on the phenomenological side of the continuum yet it also incorporates a number of aspects from the positivist side.

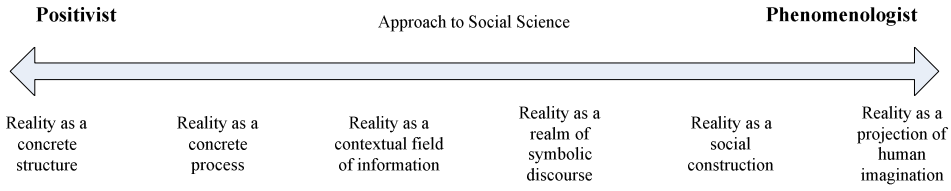

Figure 1.1: Continuum of Core Ontological Assumptions (Morgan & Smircich, 1980, p.492 in Collis & Hussey, 2003, p.51)

As illustrated in Figure 1.1 the *positivistic* and *phenomenological* approaches are two extreme research paradigms. Collis and Hussey (2003) explain that few people operate purely within any of these forms of research. The six stages identified within Figure 1.1 illustrate that many research paradigms combine a number of elements of the two extreme paradigms. Collis and Hussey (2003,

p.76) further state that, *"it is not unusual in business research to take a mixture of approaches"*. They conclude that this allows one to take a broader and often complementary view of the research problem or issue. Combining research methods is referred to as triangulation and it is argued that the underlying ontological research paradigms are not necessarily opposed, but that they can be accommodated within one study (Myers, 1997). Oates (2006, p.38) contends that *"triangulation gives researchers multiple modes of 'attack' on their research question"*.

Intermittently this research project subscribes to the view where reality is derived from the transmission of information which leads to an ever-changing form and activity. It can be argued that this approach leans towards the positivistic paradigm, as noted in Figure 1.1. However, this research project also accepts the view that the world is a pattern of symbolic relationships and meanings, sustained through a process of human action and interaction (Collis & Hussey, 2003). The latter approach is phenomenological and is particularly evident when this research project addresses the perception of trust and risk. The nature of trust and risk requires a degree of subjectivity and interpretive research, even though the researcher has attempted to be as objective as possible. Subjective and interpretive research form part of the phenomenological research paradigm (Collis & Hussey, 2003). As such, within the broader phenomenological paradigm of this research project, there are elements of positivistic philosophies of study which all contribute to enriching the research paradigm.

Nonetheless, if one research paradigm is to be singled out for this research project based on a single factor, it would be that there is no single reality or single truth of the world and that not all research approaches produce the same set of findings. Positivists subscribe to the idea that multiple lines of attack within research lead to a consistent set of findings – a single reality (Oates, 2006). Yet interpretive research tries to identify, explore and explain how all the factors in a particular study are related and interdependent (Oates, 2006).

Therefore, it must be argued that interpretive research, belonging to the phenomenological paradigm, is the dominant paradigm of this research project.

However, the researcher has been conscious of and has attempted to use logical reasoning when investigating reality where the researcher has had no effect on that reality (Collis & Hussey, 2003). Bassey (1999) agrees with Collis and Hussey, stating that positivists can explain the reality discovered to others because (a) language is an agreed symbolic system for describing reality, (b) the researchers do not expect that they themselves are significant variables in their research and (c) the events are real, irrespective of the observer.

From an epistemological viewpoint this research project embraces systems theory. This widely used and interdisciplinary concept studies the properties of systems as a whole in order to learn and understand the behaviour of systems within the real world. To summarise the concept, systems theory includes inputs, process and outputs and represents the transformation process (O'Brien, 2000). However, as pointed out by O'Brien (2000, p.21), the *"system concept becomes even more useful by including two additional components: feedback and control"*. The control element involves monitoring and evaluating feedback to determine whether a system is moving toward the achievement of its goal.

It is, therefore, essential to define the system that can be influenced by this research and distinguish between its environment and sub-systems. The rationale is that within an open system, the research project's findings are unable to influence uncertainty and trust throughout the 'entire' system. A system of controls for the management of risk can influence a sub-system, however, entropy occurs and trust cannot traverse 'several' systems without weakening as it passes through intermediaries. Likewise, continuous auditing can only be provided for a predefined system in order to provide real-time assurance.

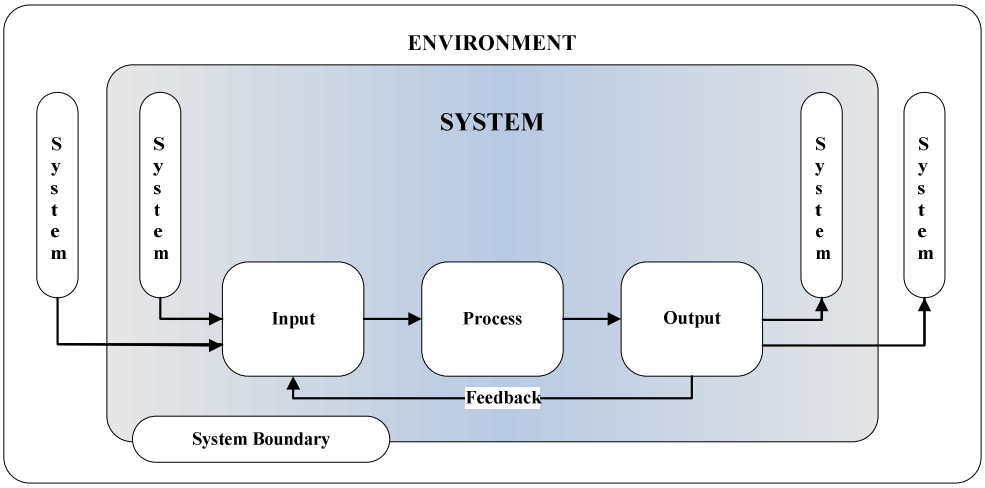

Figure 1.2: Graphical Representation of a System (Zuccato, 2005)

Figure 1.2 illustrates a system and its environment and is defined by Hanson (1995, p.27) who describes a system as *"any two or more parts that are related, such that change in any one part changes all parts"*. These parts are constructive elements in a system which together form the system. These parts represent the basic logic and functions or the process of the system. As stressed, there is no such thing as a single cause and effect relationship and that all parts of a system are interconnected.

Hanson continues and emphasises that *"any action or inaction will reverberate through the entire system leading to unpredictable effects and sometimes effects that are precisely the inverse of the intended effect"* (Hanson, 1995, p.27). This cause and effect relationship has been illustrated by the lack of investor confidence after the breakdown in financial reporting as discussed in Section 1.2. The environment represents everything that does not belong to the system and surrounds the system separating it by a 'boundary'.

To add to this, the general system theory researcher, Von Bertalanffy (1968), describes a system's view by means of a hierarchy and places a research area within this hierarchy, as illustrated in Figure 1.3 (Zuccato, 2005). A hierarchy refers to the principle to which parts or entities are meaningfully treated as

wholes and are built up of smaller parts which are themselves wholes (Checkland, 1999). This helps define the system boundary which, according to Checkland, is the area within which the decision-making process of the system has power to make things happen. The boundary distinction is made by the observer.

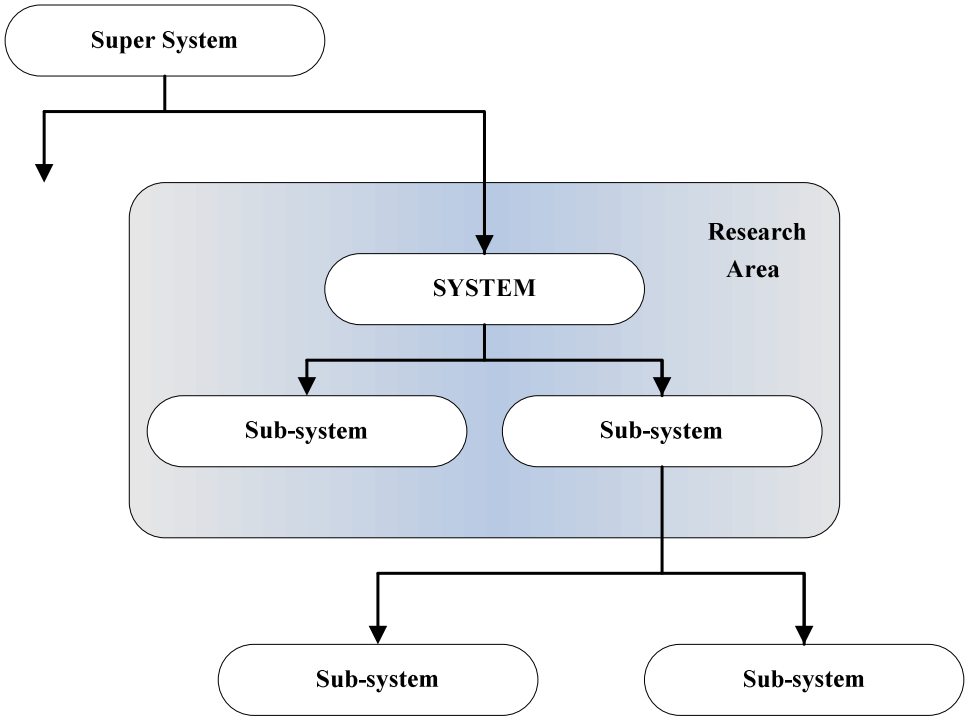

Figure 1.3: System Hierarchy with an Area of Research (Zuccato, 2005)

To reiterate, the researcher is not a potential variable in terms of this research project; hence, this research project cannot be described as pure interpretive research (Bassey, 1999; Collis & Hussey, 2003; Myers, 1997). Nevertheless, to reaffirm, the research paradigm is phenomenological biased and together with the systemic view, makes it possible to combine interdisciplinary subjects into a unified causal model.

1.5.2 Research Methodology

The notion of causality is applied where the philosophical principle of cause and effect considers the dynamics and mechanism of relationships within the system (Chia, 2002). Hanson defines causality in a system as the *"inference of relationships between things such that the combination brings about a result"* (1995, p.37). Even though existing theories have influenced this research project, inductive logic was used in the reasoning and argumentative process, followed by debating and proposing outcomes (Olivier, 2004; Oates, 2006).

This research project involved an extensive and thorough literature survey of comparable studies, frameworks, methodologies, articles, conference proceedings, standards, codes, and books (Mouton, 2001; Olivier, 2004). All attempts were made to keep the content of the research as current as possible, including the literature, which was selected from respected authorities in the field.

This led to the refining of the problem statement and the development of a conceptual causal model using modelling techniques to assist its presentation (Olivier, 2004). Furthermore it is noted that models are *"used to aid in problem understanding and solution development"* (Oates, 2006, p.108). The proposed abstract or conceptual model assists in formulating the argument, based on reasoning that stakeholder confidence can be restored within the domain of financial reporting, by providing assurances in real-time by means of continuous auditing. This is in line with Von Bertalanffy (1968, p.100) who adds that new conceptual models are often interdisciplinary and represent *"certain aspects or perspectives of reality"*.

Once the conclusions had been drawn, the overall evaluation of the project was carried out to identify errors and problems, which were then addressed. Additionally there were four papers written where the research results of this project were documented and disseminated through publications in accredited journals. Three of these papers were published in accredited journals and one

presented at a subject specific conference and published in the conference proceedings (see appendices A-D).

1.6 LIST OF CHAPTERS AND THESIS ROAD MAP

It was decided to discuss preliminary solutions throughout this thesis so as to strengthen the argument line of the research project. Thus, this thesis has not followed the traditional format of Chapters Two to Six being a literature survey followed by proposed solutions and research methodology. The solution is intertwined and embedded throughout the chapters and then summarised, culminating in a holistic solution chapter towards the conclusion of the thesis.

The first chapter is an introduction, which includes the background, identifying the problem, outlining the research objectives and research methodology. Following this, Chapters Two to Eight cover various theories and philosophies which all influence the problem (parts of the whole). Chapter Two is an investigation into corporate governance lapses, theories, principles and clearly illustrates the problem and the breakdown in control. This chapter also discusses the importance of making decisions based on sound information and then introduces control as an important facet of governance.

The third chapter is a study of trust and risk to see how these impact on uncertainty and behaviour when considering a company's stakeholders. To restore trust one needs to understand trust's relationship with risk. Additionally, this chapter proposes a trust strategy on how one can build and safeguard this concept of trust. This leads to Chapter Four which highlights that internal controls are part of risk management and information security. The concept that controls limit uncertainty and assist in managing risk is clearly explained.

Important elements of corporate governance are *fairness, responsibility, accountability,* and *transparency* (King II Report, 2002, p.19). These are discussed in Chapter Five together with the audit committee and audit profession,

which have the responsibility of providing objective and independent assurances as to the condition of the information presented within company financial statements.

Chapter Six is a pivotal chapter as it investigates how one is to determine whether the information has integrity or not. For information to be described as quality information it needs to have integrity. For the directors, managers and various stakeholders (including investors) to base their decisions on the information, they need to know that the information has not been compromised, but retains its integrity. This chapter contributes to the thesis in that it highlights the characteristics of information integrity and that both the system with the data needs to have integrity to claim that information has integrity.

The concept of continuous auditing is covered in Chapters Seven and Eight. It is argued that business decisions are made in real-time, on real-time information based on real-time information systems. The problem is that the current system of providing assurances is not in real-time. Therefore, the *mechanism* to provide assurances in real-time as to the condition of the information that decisions are based on, is a continuous auditing methodology. This section clearly explains what continuous auditing systems need to accomplish and how it is to be done.

Chapter Nine, the penultimate chapter, is a solution chapter and discusses the proposed causal model. This chapter integrates the solution components of the previous chapters and provides a holistic solution, drawing on the discussions which have taken place throughout this thesis. The final chapter, a summative conclusion, evaluates the research to determine whether the objectives were achieved and includes a discussion for further research.

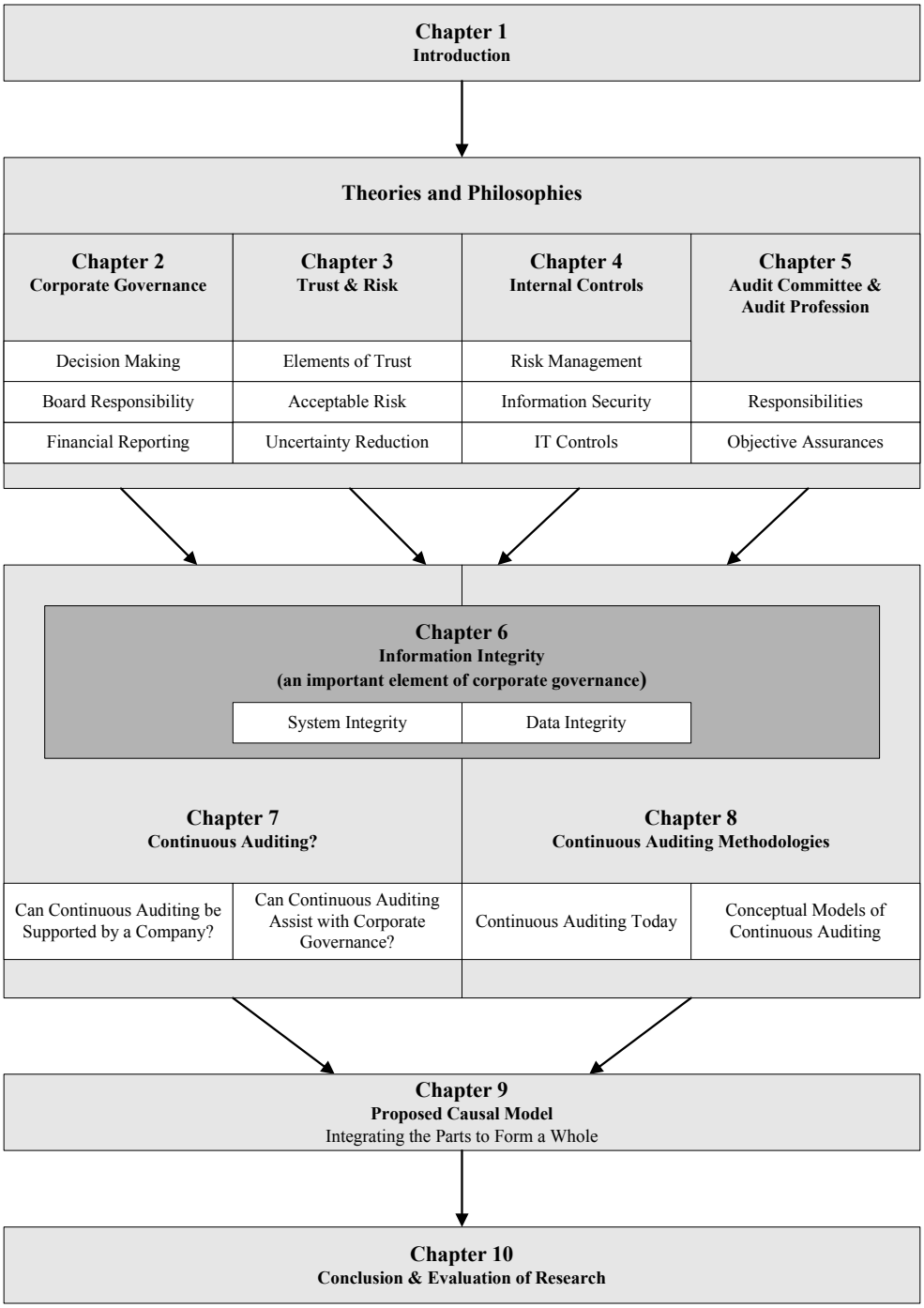

Figure 1.4: Chapter Road Map

The chapter road map, as graphically represented in Figure 1.4, illustrates the logical order of the research and where various topics are discussed in detail.

However the causal model, illustrated in Section 1.7, shows the proposed *'new idea'* and how the problem is being addressed. Olivier (2004) points out that this would be an informal model as it is not a mathematical model; however it serves as a guide if the idea were to be implemented.

1.7 PROPOSED CAUSAL MODEL

Models use constructs to represent real-world situations, essentially focussing on the problem and the solution (Hevner & March, 2003). This research project has led to the development of several concepts discussed throughout this thesis. However, Figure 1.5 is a high-level causal model encompassing the entire project. Important to note is that the model follows a top down approach, which starts with *stakeholder mistrust* as an input and the final output is *increased trust and control*.

Due to the complexity of this field of research, it has not been possible to incorporate all the detailed research findings and aspects in a single model. Considerable thought has been given to this model in order to keep it simple yet still illustrate enough so that the model is useful. This model serves to merely illustrate the high-level aspects, linking the related topics together thereby enabling a basic understanding of the chapters so that it makes logical sense when read. As noted, the causal model is used to represent the problem and the solution, which involves continuous auditing.

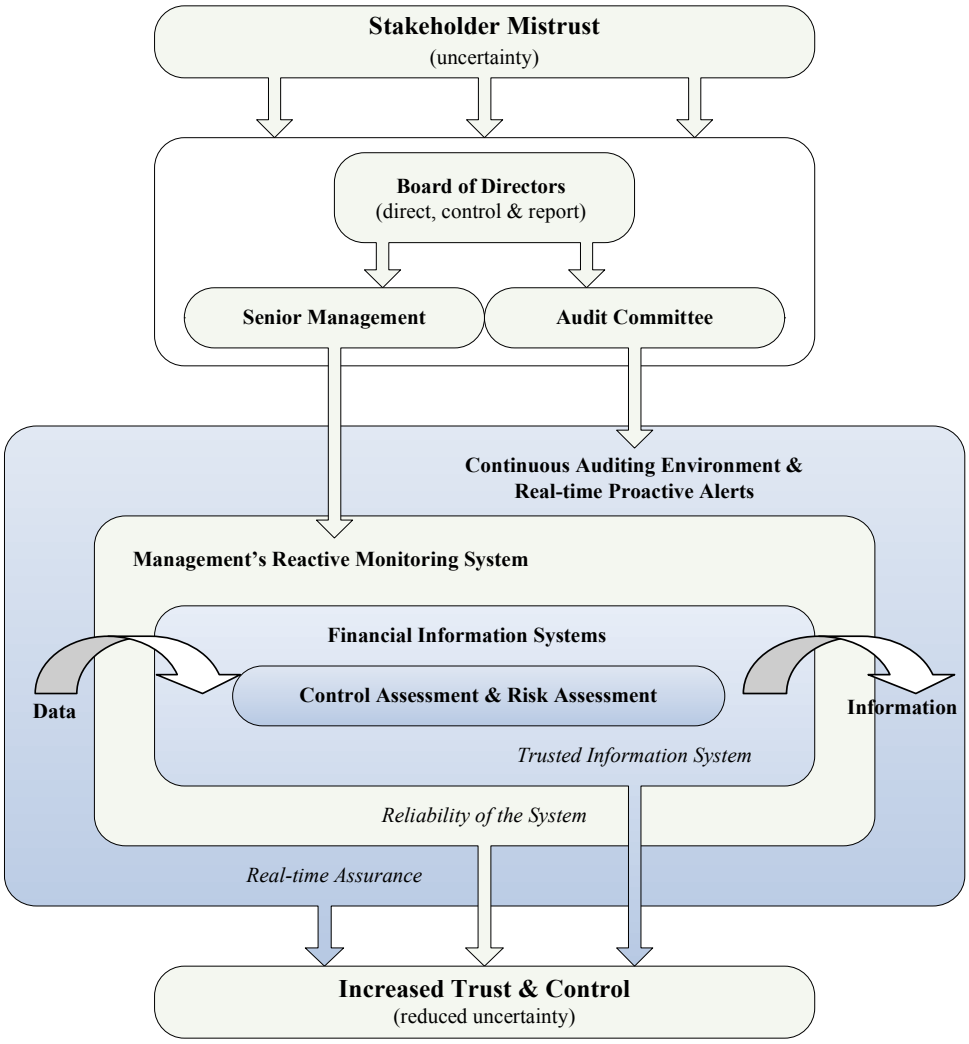

Figure 1.5: Causal Model for Increased Trust and Control

The model will be discussed again in more detail in the penultimate chapter; however, at this early stage it is essential to observe the *reactive* nature of management's monitoring system. In addition, take note of the continuous auditing environment which encompasses the entire system. The continuous auditing process has a *proactive* nature; consequently real-time assurances are more achievable than with traditional auditing methods, which are historic in nature. Also important to note is the emergent property of the model: *increased trust and control*.

1.8 SUMMARY

This research project has highlighted that in order to restore stakeholder confidence in the domain of company financial reporting, objective assurances need to be provided. These assurances should state whether the information found within the financial statements has integrity *(reliable and accurate).* This research further emphasises that the assurances need to be provided in real-time, when the information becomes available, not months after the transactions have occurred.

It also stresses that to restore confidence, both trust and controls need to be at an acceptable level. In a fast moving real-time business environment, information technology can assist in providing real-time monitoring and auditing services. This will result in providing objective *'assurances on demand'* and in real-time.

Theoretically, the intended outcomes of decisions based on the financial statements should be achieved if perfect competition exists. As such, if the fraud and errors in financial statements are eliminated, the decisions based on this perfect information should be sound and the desired outcomes achieved.

Besides addressing the issue of trust, this research project is to *'close the net'* around the financial statement debacle so that the desired outcomes of decisions, based on these financial statements, are more achievable. This will help restore stakeholder confidence and reduce uncertainty. It is an attempt to eliminate several of the risks from within the company so that the stakeholders can concern themselves more with external risk, such as market risk. Theoretically, risk will only be mitigated to an acceptable level as it is not possible to eliminate risk in its entirety. This leads to the next chapter, which is on corporate governance and highlights the cause of the problem.

Chapter 2

CORPORATE GOVERNANCE

"In theory there is no difference between theory and practice. In practice there is."

- Yogi Berra, (baseball player, b. 1925)

2.1 INTRODUCTION

Good corporate governance is of decisive importance for companies in a free, fast moving and increasingly competitive information economy. Companies need efficient structures, defining relations between the board of directors, management, investors (shareholders), and other stakeholders. Assurances need to be offered to investors that their money is being used wisely and that they have made sound investments. The balancing act of good governance is therefore to be found in the resolution of the various stakeholder's conflicting interests.

In addition, this chapter illuminates that the loss of fiduciary seriousness in the macro environment affects the tone of the company's control environment. Issues at the macro level inevitably trickle down to the micro and ultimately individual level, affecting the entire environment. The adage *'always sweep the stairs from the top down'* is central to corporate governance today. Also addressed is the important role the boards of directors play in the governance of companies. Therefore power, accountability and responsibility are discussed.

This chapter further concerns itself with several other facets of governance. These include the important topics of *governance and controls* and the foundation of decisions: *information*. The chapter introduces governance and the modern corporate form. This is followed by a brief look at *Agency Theory* and lapses in corporate governance, specifically in the area of financial reporting. It concludes with a discussion on information and information security as an important aspect of corporate governance today.

2.2 CORPORATE GOVERNANCE – AN OVERVIEW

To understand the philosophy behind corporate governance it was necessary to research the origins and follow the progression of corporate governance until its present state. It was discovered that decisions that direct and control the company are the *Achilles heel* of corporate governance, when considering the consequences or outcomes of these decisions.

2.2.1 The Origins

The word *governance* has its roots in Latin, *gubernare,* which means *'to steer, to govern'*. Originally meant to steer a ship, hence its figurative sense of *"one who guides or leads"*. It came to Latin from the Greek word *kubernan*, which means *'to steer'* (Merriam-Webster, n.d.; Quinion, 2005).

Understanding the origins of the word governance leads to a natural corollary that the board of directors is there to *'steer and govern'* the company. Sir Adrian Cadbury (2002, p.1) suggests that, *"… governance need not and should not be heavy-handed"* and this emphasises that if one is steering a ship it is the small rudder at the stern that determines the ship's direction.

The precise term *"corporate governance"* itself seems to have first been used by Richard Eells in 1960 to denote *"the structure and functioning of the corporate polity"* (Becht, Bolton & Roell, 2002, p.6). The term corporate governance itself invokes a comparison between the government of nations and that of

corporations, and the idea that the government of corporations should be akin to a democratic voting process, was in fact quite explicit in early charters of companies (Becht, et al., 2002; Dunlavy, 2004).

This is highlighted in the first *public* companies which were the East India companies. The British East India Company was granted a Royal Charter in December 1600 and was governed by a Court of Directors, 218 members (shareholders) to be precise (British East, n.d.; Cadbury, 2002, p.2). Additionally the Dutch East India Company, March 1602 is known as the first multinational company to issue shares (Dutch East, n.d.). Although four hundred years have passed, companies are still experiencing some of the same issues today: control problems, opportunism and conflicts of interest.

Today there are short-term investors versus those that take a longer view. The East India Companies had investors who wanted a return on investment after each voyage versus those that took a longer investment view. In addition, there are the various stakeholders with their own agendas and interests. Evidently there arose *'conflicts of interest'*, which is a governance issue.

Some of the most basic governance issues are those of power and accountability. Does the power lie with the owners (investors/shareholders) or with the managers and other stakeholders within the corporate system? This problem existed with the East India Companies when the boards had to control their appointees and captains who were acting, not only for the companies, but also for themselves, and were often in distant stations and out of touch for long periods of time.

It is pointed out that: *"Corporate governance has only recently emerged as a discipline in its own right, although the strands of political economy it embraces stretch back through the centuries"* (Iskander & Chamlou, 2000, p.2). Today a great deal of energy is spent on the study of corporate governance; however, it would be prudent of scholars to study and identify the *historic* principles that

underlie this discipline. It provides more depth to the understanding of the governance problems facing companies in the 21st century.

2.2.2 Corporate Governance in the Twenty-first Century

Governance as defined by The Committee on the Financial Aspects of Corporate Governance, which was chaired by Cadbury (2002, p.1), states that *"…it is the system by which companies are directed and controlled"*. Furthermore, according to Shaw (2003, p.75), the concepts of corporate governance and risk have a large overlap and have converged in recent years. Shaw argues that governance is about decision-making from available choices. He further specifies that risk is the anticipation, understanding, and action around the consequences of those decisions.

Becht, et al. (2002, p.5) contends that corporate governance is concerned with the resolution of collective action problems among dispersed investors and the reconciliation of *"conflicts of interest between various corporate claimholders"*. This is clearly understood when one considers the East India Companies with their various investors, directors, appointees and captains. The overlap of risk and corporate governance is therefore meeting the diverse needs of the various company stakeholders while attempting to achieve the company's objectives in a competitive market place. Today, many directors are aware that risk is ubiquitous in nature and needs to be carefully controlled when governing the company.

If the various stakeholders' perceived risks could be mitigated and uncertainty reduced, it would allow for an easier decision-making process as there would more than likely be consensus. This leads to a more formal and rather functional definition of governance which is proposed by the Organisation for Economic Co-operation and Development (OECD, 2004 p.11): *"Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of*

attaining those objectives and monitoring performance are determined." In other words, we can view corporate governance as a vehicle of decision-making and power allocation among investors, managers, and directors. This definition is in accord with both Shaw (2003) and Becht et al. (2002) and is a sound foundation for the definition in the King II Report (2002).

The King II Report (2002, p.19) summarises governance for the 21st century and states that, *"… there must be greater emphasis on sustainable or non-financial aspects of performance"*. This report goes on to state that: *"Boards must apply the tests of fairness, accountability, responsibility and transparency to all acts or omissions"*. In addition, boards need to be accountable to the company, but also responsive and responsible towards the company's stakeholders.

Clarke (2004, p.2) is in agreement with the King II Report and claims that corporate governance has wide implications and is critical to economic and social wellbeing. Clarke points out that governance is, first: to provide the incentives and performance measures to achieve success; second: to provide accountability and transparency to ensure the equitable distribution of the resulting wealth. The King II Report (2002, p.19) continues to state that the *"correct balance between conformance with governance principles and performance in an entrepreneurial market economy must be found"*.

In accordance with the definitions, Figure 2.1 is presented as a high-level graphical illustration. This figure shows that corporate governance is a continuous improvement process and not an event. Additionally the governance process iterates and is refined over time. The figure also emphasises the concept that the board of directors makes decisions and directs the company, in other words *guides, leads or steers*. Management implements the directors' decisions by designing and establishing business processes and a system of internal controls. In addition, management reports back to the board the outcomes of the decisions and the progress of the company. Based on the report back from management, the directors once again make decisions. However the directors'

decisions are also influenced by external factors such as regulations and the market forces. Also to be noted is the 'cause and effect' relationship that decisions have on the company. This is discussed in more detail in the following section.

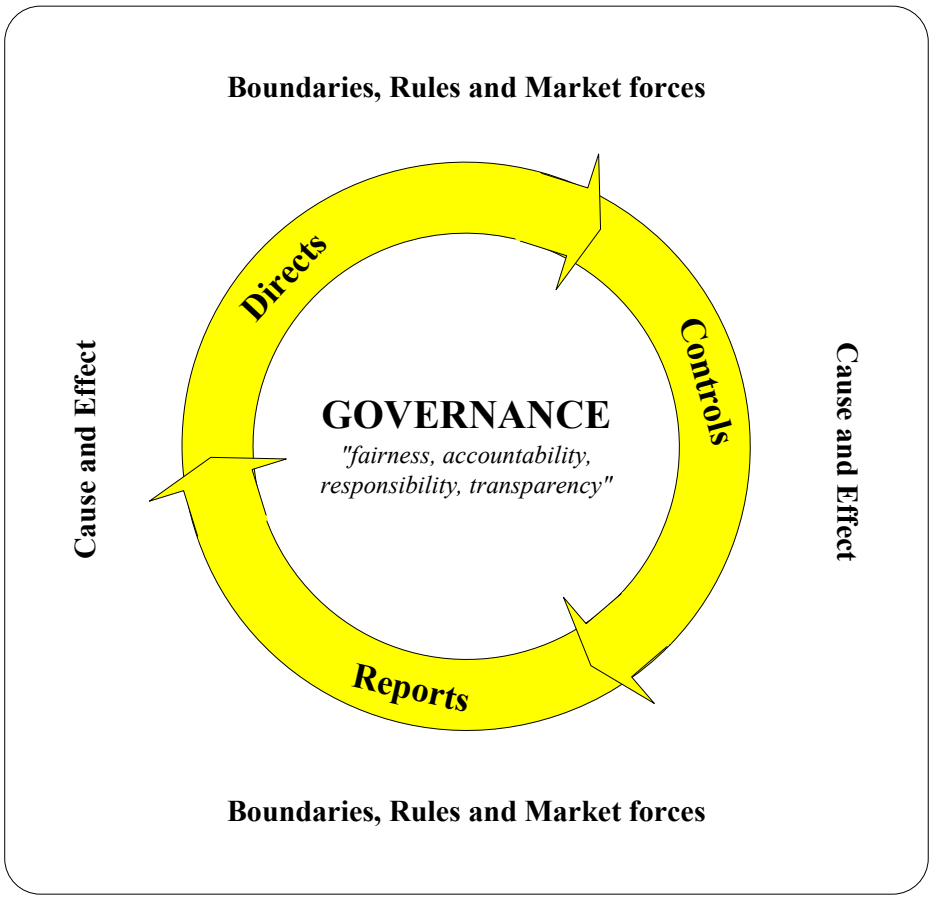

Figure 2.1: The Iteration Process of Governance

The focus of governance is therefore not on the intricacies and fine details, but rather on the direction, management oversight, control and reporting. Therefore, good governance is simply about having the framework in place to ensure that rules are obeyed and controls and responsibilities are clearly defined. For example, the rules could be laws, regulations, corporate policies, codes of practice, codes of conduct and recourse mechanisms. A governance framework

should attempt to manage risk and reduce opportunistic behaviour by applying its rules, systems and procedures.

Thus, a conclusion can be drawn as to the high-level purpose of governance. The board and management are therefore to work within boundaries and rules set by laws, regulations, policies and the various stakeholders, including the providers of funds. These boundaries and rules are often changed and the key is to direct *(steer and govern)* the company so that the desired objectives are obtained in a controlled way. This needs to be done while *managing the company's risk exposure* and taking into account market forces.

2.2.3 Decisions have Consequences as One Directs

As noted, an important part of governance is accountability and responsibility. In other words, dealing with the consequences or outcomes of one's decisions. It is no longer acceptable for the board, or senior management, to say *'I did not know'* when something goes wrong. The ignorance argument is no longer acceptable and *due-diligence* is expected. Due-diligence, being defined as *"a term describing a thorough effort to intercept potential problems"* (Integrity Incorporated, 2005) or the care a reasonable person should take before entering into a transaction (Free Financial Dictionary, 2005).

Decisions, together with their consequences, could be better understood if Jonas Salk's statement is pondered and considered together with the subsequent paragraphs. Salk stated that: *"The most fundamental phenomenon in the universe is relationship"* (Smith & Fingar, 2003, p.7). Expounded upon by Woods (n.d.) and applied to a company setting, it is noted that everything influences everything in one way or another. Whether the board members or senior management are aware of this or not, does not change the fact that it happens. This view is in harmony with this research paradigm which was introduced in Chapter One (Section 1.5.1). Woods stresses that a company is a system and that any action will reverberate throughout the entire company. In science this relationship is known as *'cause and effect'* and has been traced back

through many centuries to the ancient Greek, Aristotle, who taught this concept (Hanson, 1995).

In accordance with the cause and effect principle, Shaw (2003, p.30) draws attention to the importance of decisions, choices and their subsequent consequences when one considers corporate governance and risk. Shaw points out that the failure to anticipate and understand the consequences of choices and decisions is a problem many board members face.

For three hundred years the world attempted to solve problems the way Sir Isaac Newton viewed the universe. A summary of Newton's theory is that the universe consists of countless uniform particles held together by gravity. The universe was viewed as one big machine and that all the homogenous particles forming this mechanical view, not only fitted together, they moved together without regard for space and time (Spielberg & Anderson, 1987, p.50). To understand a problem it needed to be broken down into its component pieces, the pieces repaired, and the *machine* put back together again.

Today board members need a paradigm shift from Newton's theory to the fundamentals of Albert Einstein's theory. Einstein proved Newton's perspective incomplete and introduced the world to quantum physics/mechanics, atoms and molecules. Einstein's *Theory of Relativity* (Einstein, 1961), explains time and space, and the notion of the observer and the observed (being part of what one sees). Simply stated the Theory of Relativity is that everything has an effect on something else. Nothing is done in isolation as everything is linked. This is in harmony with Aristotle who introduced the idea that the *whole* is greater than the sum of its parts. Hanson (1995) adds that to view the world through this lens clearly illustrates a cause and effect relationship and that the *parts* can have a causal effect on each other. This was discussed in Chapter One when discussing systems theory (Section 1.5.1).

Therefore one can conclude, when the theories of Salk, Woods, Hanson, Shaw and Einstein are considered, that every choice or decision a director makes, and follows through with, will have consequences for the company. Even if these consequences are not immediate, they still affect the various company stakeholders at some stage. Thus, to assist the directors in the decision-making process, in accordance with the governance definitions *(that governance can be viewed as a vehicle for decision-making)*, there is the need for *controls to guide* the decision makers' decisions so that the desired outcomes of the decisions are achieved.

2.3 CORPORATE GOVERNANCE AND CONTROL

An important component of corporate governance is control. If one is to steer or govern, one controls the direction of the company. This leads to the next section on the details of the corporate form and responsibilities of the CEO and the board of directors. Agency Theory is discussed as it highlights the conflicts of interest that exist in the modern corporation. This section concludes by arguing that the current governance structures have failed and increased control and accountability is required.

2.3.1 The Corporate Form

The corporate form was created as an entity that could outlive any of its members and the board structure was established by law as a vehicle to ensure its continuity and to fix a locus of responsibility for control (Zald, 1969). The board is generally viewed as fulfilling its formal responsibilities, supported by the legalistic argument, which indicates that directors must exercise reasonable business judgment in the interests of the shareholders while remaining loyal to the interests of the company (Budnitz, 1990). Although the law gives the board the formal power to control the company, it provides no specific method to do so (Carpenter, 1988; Ong & Lee, 2000).

The method whereby the board then chooses to exercise its formal power to control the company is through the appointment of an *agent* to run the company, i.e. the Chief Executive Officer (CEO) (Eisenhardt, 1989; Jensen & Meckling, 1976; Spatt, 2005). The CEO then develops a system of management through which decisions are made and carried out.

Nevertheless, regardless of the method of management and controls, the board retains its formal authority over management and is *responsible* for the company's conduct and performance (King II Report, 2002; OECD, 2004; Tricker, 1994). To emphasise the point: the day-to-day responsibilities of managing the company are left to management; however, the board retains ultimate authority and responsibility for the company's performance (Flowerday & Von Solms, 2005b).

It should be noted that the company exists as an entity to provide value for stakeholders (COSO-ERM, 2004). If the company does not add value within the value chain, market forces will eliminate the company from the chain. Furthermore, it is stressed by Donaldson (2005), the chairman of the Securities and Exchange Commission (SEC) in the USA, that capital will flee environments that are unstable or unpredictable and that investors must be assured that companies are living up to their obligations. Hence, the board together with their system of management are required to *control* the company's activities and provide value to the company stakeholders, demonstrating that the company is living up to its obligations.

2.3.2 The Board of Directors

Boards are generally composed of a chairman and three types of directors including the managing director, non-executive directors and executive directors. The managing director of the company is often the CEO and sometimes the chairman. Non-executive directors are considered independent of the CEO and therefore more objective in decision-making (Cadbury, 2002, p.50; King II Report, 2002, p.57; OECD, 2004, p.58). The final category, executive directors,

is a category of directors including current or former members of management, and is generally thought to lack objectivity or power to challenge the CEO (Bradshaw & Jackson, 2001).

One of the board's roles is that of monitoring the actions of the CEO (Walsh & Seward, 1990). Internal control mechanisms include the monitoring of managerial behaviour by the board of directors and incentive alignment through such things as performance-based compensation. Boards of directors are designed to give permanence to the oversight of management, a concept raised by *agency theory*. Having effective boards of directors to oversee the investment of shareholders' money is essential for investor confidence (Leblance & Gillies, 2003). Accordingly, one concludes that the board has the responsibility to *control* the CEO and management so that the company's desired and agreed upon objectives are achieved in harmony with the boundaries and rules set.

2.3.3 Agency Theory (the Principal and the Agent)

As noted earlier, conflicts of interest exist between the various company stakeholders. This was highlighted as early as 1776 in the milestone writings of Sir Adam Smith (1981, p.741). He cautioned that directors are managers of other peoples' money (investors' money) rather than their own money. Smith warned that it cannot be expected that directors look after the money as conscientiously and with as much vigilance as private partnerships or individuals watch over their own money.

Whilst this discussion of corporate control *(power and accountability)* goes back to the emergence of the publicly owned company, however, and as pointed out earlier, the research on corporate governance is more recent. Most reviews of corporate governance trace the origin of the field back to the work of Adolf Berle and Gardiner Means in 1932 (Berle & Means, 1967). Berle and Means placed the problem of the separation of corporate ownership and managerial control at the centre of the discipline. This development has placed this classic *principal-agency* problem at the forefront of most researchers' concerns.

Since the company's share price is normally related to a company's performance, the return to investors is dependent on how well a company is managed. A company's professional managers serve as agents for shareholders by making decisions that are supposed to maximise the company's value. The separation of *ownership* (investors) and *control* (managers) can result in agency problems because of conflicting interests. This is not too dissimilar to the East India companies which illuminated the governance issues of control, conflicting interest and opportunism four hundred years ago.

Managers may be tempted to serve their own interests rather than those of investors who own the company's shares. Investors rely on the board of directors of each company to control and ensure that its managers make decisions that enhance the company's performance and maximise the share price. Therefore, the board of directors is charged with representing the investors' interests and at the same time remaining loyal to the company (Budnitz, 1990). An example of a conflict is when the investors may want a larger dividend payout which may not be in the company's best interest or the directors want larger bonuses yet the company's share price and performance may have declined. This could be because the various parties are seeking short term rewards?

This is why fairness, accountability, responsibility and transparency, which are emphasised by the King II Report (2002), are of such importance. Additionally, the point Shaw (2003) makes that directors need to see further down the line and anticipate what the outcomes of their decisions may be *(due-diligence)*, is of utmost importance. Once again this links back to the control aspect, or the need to assist in controlling the decision-making process so that the desired and agreed upon objectives are achieved.

2.3.4 Failure of Current Governance Control Structures

From this literature survey it has been found that studies have suggested financial markets reward companies with strong monitoring, control and good governance mechanisms. The same studies have shown that the financial markets punish those with weak ones (Bai, Liu, Lu, Song, & Zhang, 2004; King II Report, 2002, p.12; Westphal & Zajac, 1998). The literature on corporate governance operates on the premise that agency problems inherent in modern companies can be minimised by the use of appropriate control and monitoring mechanisms, and in turn, should lead to desired behaviours and higher performances (Eisenhardt, 1989; Jensen & Meckling, 1976; Spatt, 2005). Much of the existing research on corporate governance has taken this efficiency oriented perspective, where governance structures are chosen as contracts that minimise both potential agency costs (i.e., costs associated with conflicts of interest between owners and managers) and the costs associated with the use of internal control mechanisms (Zajac & Westphal, 1994).

However, with the sheer number of blatant transparently poor decisions exhibited by many company executives and directors and the systematic failures of governance structures in cases such as: Enron, Parmalat, Tyco, WorldCom, Arthur Andersen, Computer Associates, Global Crossing, Lucent Technologies, Adelphia, Xerox, Saambou, Labat, Bearings Bank, Halliburton, KPMG, China Aviation Oil, Merrill Lynch, Disney, and Ahold to name just a few, suggest the use of poor judgement and lack of *due-care*. Due care is defined *"as the care that a reasonable man would exercise under the circumstances"* (Free Legal Dictionary, 2005) or the conduct that a reasonable person will exercise in a particular situation, in looking out for the safety of other parties (Law.Com Dictionary, 2005a). Due care is a way of testing if *negligence* is present.

The following is a list illustrating more detailed examples of the failures in the corporate governance structures in recent years:

- An investigation of Enron uncovered multiple *"off the books"* transactions with related entities, risky accounting practices,

excessive compensation, and financial ties between the majority of *outside* board members and the company (USA Senate, 2002). Enron was also named America's most innovative company by Fortune Magazine for six consecutive years and then suddenly and in only 46 days, Enron's share price fell from US$90 to 30 cents per share as the accounting scandals were discovered (Gilbert, 2006).

- Dennis Kozlowski, former Tyco CEO is currently on trial for allegedly defrauding the company's shareholders out of US$600 million together with Tyco's CFO, Mark Swartz. This includes a US$2.1 million birthday celebration for Kozlowski's wife on the island of Sardinia (Jurors see tape, 2003; Lowenstein, 2003a).
- Dick Grasso's US$139.5 million pay package at the NYSE (Lowenstein, 2003a; Tully, 2003). While the exchange requires NYSE companies to follow SEC regulations by fully disclosing the pay of its top officers, the NYSE kept its boss's huge compensation a total secret, even from the SEC and the owners of the NYSE.
- Many executives of the over-valued telecommunications companies cashed in over US$6 billion in the year 2000 yet they touted the sector's growth potential just as it was about to collapse (Clark, 2004, p.15).
- WorldCom's board signed off on financial statements that had overstated profits by US$7.1 billion between 2000 and 2003. Clifford Alexander Jr., who left the board in January 2002 after missing half the meetings in 2001, is chairman of Moody's Investors Service, which failed to downgrade WorldCom bonds until April 2002 (Clarke, 2004, p.16).
- Parmalat's shares were suspended in December 2003 after it was found that the directors were hiding Euro14.5 billion losses in a *"hole in its books"* and the company was actually insolvent (Parmalat sues, 2005).
- The 1998 Russia / East Asia / Brazil crisis. The crisis known as the East Asia crisis highlighted the flimsy protections investors in

emerging markets have. It is no coincidence that corporate governance reform in Russia, Asia and Brazil has been a top priority for the OECD and World Bank (Iskander & Chamlou, 2000).

- Merrill Lynch, one of the world's largest stockbrokers, agreed to pay US$100 million to settle a claim and agreed to reform after its analysts were caught persuading customers to invest in Internet shares they knew were worthless. This was done to bolster the company's revenues and their own commissions (Hodge, 2002).
- Saambou, one of South Africa's largest banks, was placed under curatorship and then bankruptcy in a surprising move amid allegations of fraud and insider trading by directors; the investigation is still ongoing (Mittner, 2003; Mittner, 2005). The total sum of money involved in the alleged offences is R640 million. The three co-accused are De Clercq, the general manager, along with Myburgh and Edwards who were both executive directors (Saambou execs, 2005).
- It is estimated that Russians paid US$316 billion in bribes to police, licensing bodies and state inspectors during 2004 (Bribery in Russia, 2005). The article succinctly sums the situation up by stating, *"when the bureaucracy isn't controlled it starts to earn for itself"*.
- The African Union claims that corruption is rife within Africa and that both public and private sectors are involved. It is estimated that as much as 25% of Africa's gross national product or $148 billion is lost per annum to fraud and corruption (Corruption costs, 2006).
- Gary Smith, CEO of Ciena Corporation which supplies communication and networking equipment, received compensation of US$41.2 million for the last four years. However, the company's shareholders wealth has virtually been obliterated – losing 93% of the share value during the last four years. In the same period where the CEO was paid a fortune, the investors have lost almost all their money (Brush, 2005).

These have just been a few examples to illustrate the gravity of the situation. Phillips (2003) claims that the mentality of greed gave us the likes of Enron and WorldCom. He goes on to illustrate how the ten highest compensated executives in the USA had an average annual compensation of US$3.45 million in 1981; however, in 1988 the average annual compensation for this group had climbed to US$19.3 million. In 2000 it had soared to US$154 million per annum.

It appears that many members of executive management and the board of directors have wilfully breached their fiduciary duties in order to defraud investors for personal gain. This *opportunistic* behaviour allowed them to profit greatly by engaging in unethical practices, and thus managerial greed, which caused the governance structures to fail (Charan & Useem, 2002; Lowenstein, 2003b; Nisenzoun, 2004; Smith, 2005). Alan Greenspan (2002), Chairman of the US Federal Reserve Bank, referred to this as *"Infectious Greed"*.

It is clear that the existing efficiency based explanations of corporate governance failed. These failures included: *"auditing lapses, hiding loans or losses, insider trading, and inflating revenue"* (A Question of, 2002). Additionally, there are information security breaches which companies have attempted to control and mitigate to an acceptable level for decades; however, these too have been on the increase. According to a survey by the FBI in America, 90% of their respondents had detected information security breaches within the previous twelve months (Stair & Reynolds, 2006). Consequently, one can conclude that to practise good governance today, increased accountability and transparency plus a robust system of controls is required.

2.4 THE REACTION TO THE CORPORATE GOVERNANCE FAILURES

This has had an adverse effect on company investors (the owners of the company's shares). Many investors have disposed of their shares and this has affected the companies' market capitalisation. In fact stock markets across the

world plummeted in the early part of this millennium. For example, the NASDAQ's combined value from its high point to its lowest point dropped by 77.8% (Walker, 2003). Company investor confidence (stakeholder confidence) is slowly being restored; however, it is still below the highs of the year 2000. This section highlights the effort by governments, regulators and professional bodies to restore stakeholder confidence. In addition, the section concludes with a discussion on financial reporting which has been at the core of the governance failures.

2.4.1 The Spawn of Corporate Governance Codes

In an effort to minimise future corporate governance failures, there has been a plethora of laws, guidelines, codes, principles, standards and regulations spawned. From this point on these collectively will be referred to as *codes*. A natural question to ask then is why codes imposing particular governance boundaries and rules (required by stock exchanges, legislatures, courts or supervisory bodies) are necessary? This question is peculiar because it is in the interest of companies to provide adequate protection to shareholders.

Becht, et al. (2002, p.21) claim mandatory governance boundaries and rules are necessary for two main reasons; firstly, to overcome the collective action problem resulting from the dispersion among shareholders; secondly, to ensure that the interests of all relevant stakeholders are represented. After reading a number of these codes it is quickly revealed that their dominant focus is on boards and board related issues as well as responsibilities that the directors should be addressing.

From the literature survey it was found that the publication of the Cadbury Report and Recommendations (1992) in the UK spawned the proliferation of codes. This list is far from inclusive and is continuously growing, however, it does include:

The King I & II Reports (1994 & 2002, South Africa), OECD Principles of Corporate Governance (1999 & 2004, thirty countries are members of the

OECD), Vienot Reports I & II (1995 & 1999, France), following Cadbury in the UK there was amongst others Greenbury (1995), Hampel (1999), Turnbull (1999, 2005). The USA has legislated corporate governance with the Sarbanes-Oxley Act of 2002. A comprehensive list of *codes* from across the world is far too numerous to list in this research project (see the ECGI for list, n.d.).

Compliance by companies to the applicable *codes* has become a focus area in recent years. Since members of the board of directors are attempting to improve their governance structures by complying with these codes, there has been a noted increase in focus on financial reporting and the controls surrounding the financial processes.

2.4.2 Financial Reporting

Many of the accounting irregularities and scandals that enabled companies to vastly overstate their earnings and hide losses often emerge during economic downturns: as J. K. Galbraith (Cornwell, 2002), the eminent retired Harvard University professor once remarked, *"recessions catch what the auditors miss"*. However true this statement is, it has proved to be too late as it is comparable to closing the stable door after one realises the horse has bolted.

This has led to a loss in stakeholder confidence in the board of directors and the auditing profession in the domain of company financial statements. The current system of controls and assurances has failed because independent assurances are provided *ex post* and are historic (Flowerday & Von Solms, 2005b). Consequently, by the time all the stakeholders have the independent and objective assurances from the auditors as to the condition of the information presented in the company financial statements, the irregularities and scandals have occurred and it is too late.

In addition, the directors and managers make decisions in real-time as business is conducted in real-time and the information they base their decisions on is provided in real-time. Therefore, there is a need to provide assurances in real-

time (Alles, et al., 2005; Flowerday & Von Solms, 2005a; Onions, 2003). Without real-time assurances they could unknowingly be steering and governing the company in the wrong direction. Therefore real-time assurances will help identify intentional and unintentional errors when they occur and not months later.

An American response to the lapses in corporate governance has resulted in the influential Sarbanes-Oxley Act of 2002, which was passed in an attempt to help restore investor confidence. The Act further aims to enhance corporate governance and strengthen corporate accountability. This Act has been the most significant piece of securities legislation passed in the USA since the securities acts of 1933 and 1934 (Donaldson, 2005; Morrison, 2004). This Act, as with the Basel II Accord for banking, augment the need for systems of internal and disclosure controls on financial and operational processes. The Act (2002, p.1) states that it is *"to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes"*.

This represents a shift from disclosure-based legislation to more transparent substantive regulation of procedures, processes and practices (Morrison, 2004). Disclosure requirements in the past have required that companies publish audited financial accounts and they are to report market sensitive information to their investors in a timely fashion (Lundholm, 1999; Pitt, 2002). Substantive regulation goes further and requires that the law governs rights and obligations of those subject to it. In addition, it establishes *principles* and creates and defines rights limitations under which one is governed (Morrison, 2004; Pitt, 2002; Law.Com Dictionary, 2005b).

The Sarbanes-Oxley Act establishes requirements for the SEC in the USA to establish rules to which public companies comply. Among these rules and safeguards are the following important points relevant to this research project:

- The *CEO* and *CFO* are to certify the company's internal controls over financial reporting (Section 302 of the Act). Note that it is not just the figures in the financial statements, but also the controls over the financial reporting processes. This section ensures that the responsibility and accountability is shared by the very top of the company.
- *Auditors* and *management*, in their assessment of risks, are to certify the *adequacy* as well as evaluate and report on the *effectiveness* of internal controls over financial reporting (Section 404 of the Act). There were 582 companies which made *"weakness and deficiency disclosures"* during their 2004 filing of financial statements in the USA (582 weakness, 2005). The majority of these disclosures, 50.1%, were related to financial systems and procedures.
- *"Material changes"* are to be disclosed to the public on a real-time basis. This is broadly defined as all significant internal control design or operational deficiencies that could adversely affect the reported financial information and is to be done for the protection of investors (Section 409 of the Act). It is expressed that this be carried out on a *"rapid and current basis"*. There are those who stress that this section is of utmost importance to the investor and that it will create a challenge for the *IT* community to comply with as this requires a dynamic risk monitoring framework (Emery, 2004; Morrison, 2004). As emphasised, real-time reporting requires real-time assurance (Alles, et al., 2005; Flowerday & Von Solms, 2005a; Onions, 2003).

Non-compliance to the Sarbanes-Oxley Act for companies listed on US stock exchanges results in significant penalties for CEOs and CFOs, including monetary fines and/or imprisonment. The USA is not alone in passing legislation in an attempt to improve stakeholder confidence and improve corporate governance. As highlighted, the world securities markets have recognised the need for reform.

Donaldson (2005) stated that the standards everywhere are being raised to ensure that the investors have the protection they need and deserve. This is evident in regulations similar in nature and intent to the Sarbanes-Oxley Act, being considered and passed in many countries, for example, South Africa, Canada, Australia, Singapore and the European Union. The various codes, including legislation, are to ensure that the information found within the financial statements is both *reliable* and *accurate* and can be *validated* by the auditors. This stresses the importance of having current and correct information.

2.5 INFORMATION AND CORPORATE GOVERNANCE

"Information is the oxygen of the modern age." (Ronald Reagan, past President of the USA; 1996). The world has moved into the *information economy*, an economy based on the exchange of knowledge and services rather than physical goods and services (Australian Government, 2001). Reliable and accurate information has truly become crucial to effective decision-making and meeting company strategies and objectives. This section examines information assets, followed by information security and information integrity as important aspects of corporate governance.

2.5.1 Information Assets

Information held by a company's information systems is among the most valuable assets in the company's care and is considered a critical resource, enabling the company to achieve its objectives. Accordingly, it is stressed that IT products or systems ought to perform their functions whilst exercising appropriate control of this digital information and to ensure it is protected against accidental or deliberate *dissemination*, *modification*, or *loss* (Common Criteria, 2004; Ward & Peppard, 2002). The NIST 800-53 Publication (2005) includes in its assessment of risk a more holistic definition, which includes *access*, *use*, *disclosure*, *disruption, modification*, and *destruction* of information.

In fact, it has become so important to protect a company's digital information that the board itself has a fiduciary *"duty of care"* to ensure that information assets are properly protected (King II Report, 2002; Sullivan, 2000; Turnbull Report, 1999). In addition to due-care, there is the legal responsibility of compliance with laws and regulations (Westby, 2004). If the information becomes compromised in any way, it will affect the decisions based on this information and undesirable outcomes from those decisions may occur (as noted in Section 2.2.3 discussing cause and effect). This would lead to a negative perception of the *value* of the information held by the company's information systems.

The Brookings Institute's research and Baruch Lev's analysis of the Standard & Poor's 500 companies (Lev, 2001) suggested that by the late 1990s, on average, 85% of the market value of companies resided in intangible assets (brands, reputation, information, human capital) – *"the largest part of those intangibles being information*". The remainder of the company's value, approximately 15%, resided in tangible assets (fixed property, factories, vehicles).

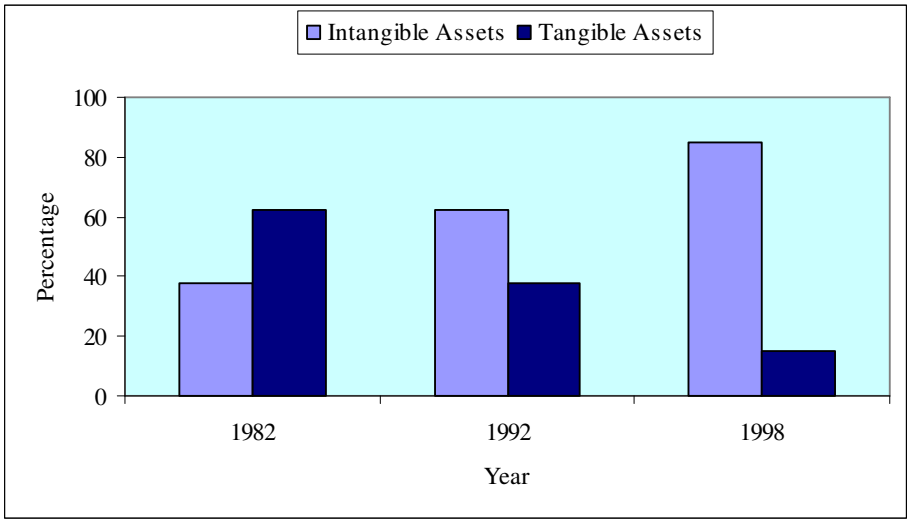

Figure 2.2: Percentage of Company Market Value Related to Tangible and Intangible Assets (Brookings Institute & Baruch Lev's Analysis)

There has been a significant shift in the valuation of companies from the early 1980s to the late 1990s as the world has advanced into the information economy, as shown in Figure 2.2. One of the driving forces behind this shift in market valuations of companies could be the need for increased investment performance. However, regardless of what the driving forces may be, to ensure that information retains its worth it needs to be secured and the users need to have confidence when basing their decisions on the information (Flowerday & Von Solms, 2005a).

2.5.2 Information Security

As explained by Flowerday and Von Solms (2005a), *"information security is an all or nothing proposition"*. For example: are the horses in the field 75% secured if a fence exists only on three of the four sides? Obviously the horses are not secured. In securing information assets and conducting business electronically, information security is raised from a technical issue to a business issue (Dang van Mien & Green-Armytage, 2002). This accentuates the need for *"embedding risk and control"* within the culture of the company (Wilson, 2002). Ultimately the board of directors should ensure that management take the necessary steps to protect the company's information assets.

In accordance with the above statement, information security has in fact become a corporate governance challenge and therefore requires all levels within the company to be conscious of the vulnerabilities and risks facing the company (Conner & Coviello, 2004; Conner, Noonan & Holleyman II, 2004). This has been heightened by many governments around the world passing new legislation concerning the safety of information.

The objective of information security is *"the protection of the interests of those relying on information"* (Horton, et al., 2000). To illustrate the importance of this, the AICPA's (2005) Top Technologies Survey showed that for the third consecutive year America's number one technology concern is "*information security"*.

The NIST 800-53 Publication (2005) points out that information security is preserving the *availability*, *confidentiality* and *integrity* of the information system resources. This is in harmony with ISO/IEC 17799 (2005), which serves as a sound security standard for many companies. ISO/IEC 17799 has information *integrity* as one of the three central pillars of securing corporate information assets along with *confidentiality* and *availability*. It is also stated within this standard that assurance is attained through controls that management creates and maintains within the company. Therefore, companies today have a system of internal controls that help mitigate the risks to an acceptable level when securing their information assets.

Thus, it is imperative that the information the board and management base their decisions on is *reliable* and *accurate*. If the information has been tarnished, it will affect the decisions based on that information and therefore the outcomes of those decisions. In addition to the board and management being responsible for the outcomes of their decisions (consequences), they must ensure the company's information is secure and protected in a controlled way. Hence, if the directors are to be found practising good governance, they will ensure that the management of the company protects the information assets.

2.6 CONCLUSION

From the literature survey, it has been noted that there has been an explosion of research on the topic of corporate governance in the past two decades. If there is one point on which most researchers agree, it is that corporate governance is a pillar of wealth creation and is the responsibility of the board of directors. The Asian and Russian financial crises of 1998 or the recent collapses of companies such as Enron, WorldCom, etc. have highlighted the fact that poor or corrupt corporate governance practices worsen investor confidence.

In addition, the literature has shown that CEOs at times *'cook the books'* in order to support share prices and their own bonuses. This is a major conflict of interest and a principal-agency problem. It has also shown that boards of directors are weak and ineffective monitors of managers. This board weakness has called for additional mechanisms for monitoring and controlling management. Because of the governance failures, there has been a plethora of *codes* spawned in an attempt to protect the investor and help restore stakeholder confidence.

The literature survey has also revealed the importance of sound and secure information assets. It is of utmost importance that the financial information is reliable and accurate and has integrity so that the decisions based on the information are sound and enable the company to achieve its objectives. The decision makers need to make decisions confidently, knowing that when they *'steer and govern',* uncertainty is at an acceptable level and there are controls in place to guide them.

To restore stakeholder, in particularly investor confidence, trust needs to exist between the stakeholders. The investors need to trust the members of the board of directors to present *reliable* and *accurate* information in the financial statements. In addition, as required by the codes, increased transparency and an adequate system of internal controls is required. The concept of trust, risk and uncertainty reduction will be discussed in the next chapter.

Chapter 3

RESTORING TRUST

"Ha, ha! What a fool Honesty is! and Trust his sworn brother, a very simple gentleman!"

- William Shakespeare, (The Winter's Tale, act 4, sc.3, 1.)

3.1 INTRODUCTION

When conducting the literature survey, it was found that there was a lack of research specifically addressing the concept of trust in a corporate governance setting. This is especially so when focussing on financial information, the board and its relationship with the various company stakeholders. Therefore, it has been necessary to draw from the work in other research disciplines to extend the study of trust to this domain. When conducting this study, it was felt that uncertainty reduction, trust, risk and behaviour all contribute to a deeper understanding of the research problem being addressed. Additionally, this chapter argues that mutual assurances assist in building trust and that information security assists in safeguarding trust.

As discussed in the previous chapter, an important element of corporate governance is the safeguarding of corporate information. This research project however, takes a narrower view and specifically focuses on information found within the financial statements and the data that make up this information. It is the board's responsibility to ensure that this information is correct and that the information's integrity is intact, even though management may see to the operations thereof. However, it has been shown that this is often not the case and

the information does indeed lack integrity. This consequence has led to two interrelated problems. Firstly, a lack of stakeholder, especially investor, confidence exists as a result of a lack of trust in the board of directors in the domain of financial reporting. Secondly, the decisions based on this information by the various stakeholders, including the managers, may be flawed due to substandard financial information.

The following facets of trust will be addressed in this chapter. Firstly, Uncertainty Reduction Theory and its relationship to trust. The discussion moves to what trust is, including a triad of elements that contribute to the concept of trustworthiness (Mayer, Davis & Schoorman, 1995). Does one trust the other party's *Integrity*? Does one trust them to have *Benevolence*? Finally, does one trust their *Ability*? The board of directors and those responsible for producing the financial statements need to be perceived as trustworthy. This highlights that trust is domain specific; for example, one may have integrity and not ability. Therefore, the board may be trusted in the domain of integrity/honesty, but not in the domain of ability/competence.

Additionally and importantly to be discussed, is the relationship between trust and risk and the effect it has on behaviour. Furthermore, trust is an important element of security and in return, security helps safeguard trust. What is more, trust and controls are both needed to establish confidence. If one considers that an important part of the communication process between the board and their investors, as to the state of the company, is via the financial statements, then it becomes imperative that the information found within the financial statements is trustworthy. When decisions are based upon this information they must be made with confidence. Finally, several aspects are proposed to help build and safeguard trust.

This chapter contributes an important point to this research project. The point is that assurances are required to build trust and information security is required to safeguard trust (Flowerday & Von Solms, 2006). However, assurances provided

months after transactions occur, are not sufficient. Therefore, to reduce uncertainty, as discussed in the Stag Hunt game (game theory), assurances are required in real-time. These assurances need to confirm that the information provided is both *reliable* and *accurate*.

3.2 UNCERTAINTY REDUCTION THEORY

Situations arise where stakeholders, including investors, need to trust the board of directors in the domain of financial reporting. Financial statements are approved by the board of directors and compiled by company staff members responsible for preparing the statements on behalf of the company. However, the problem is that these formal company financial statements are produced months after the transactions have occurred.

In addition, the stakeholders, including managers, make decisions based on real-time financial information they receive on a regular basis from real-time accounting information systems. These decisions are made without assurances as to the condition of the information on which they base their decisions. Yet they are held responsible for the outcomes of these decisions. It is therefore important to note that the various stakeholders may not be aware of how often they make trusting decisions, based on current/real-time information, without assurances. As stated, the assurances are often provided months after the transactions occur and due to this, the level of uncertainty affects the decisions made. Uncertainty reduction and perceived trustworthiness act as a precondition of behavioural trust, which involves risk in a vulnerable situation.

3.2.1 What is Uncertainty Reduction Theory?

The original Uncertainty Reduction Theory by Berger and Calabrese focused exclusively on the potential influence of uncertainty and the reduction of uncertainty during the beginning of a relationship (Sunnafrank, 1986). The theory revolves around reducing uncertainty and increasing predictability about the behaviour of various parties. Berger and Calabrese (1975) emphasise that

through communication and the exchange of information about each party, a decrease in uncertainty occurs.

According to Berger's definition (1987, p.41) uncertainty about the other party is the *"(in)ability to predict and explain actions"*. Even though their study dealt with individuals and their behaviour, the principles are relevant to the board of directors and their relationship with the various company stakeholders. The reason for this is the various stakeholders, especially investors, do not wish to be caught off guard, but need to have reasonable assurances that their expectations will be met. Uncertainty is reduced by generating and confirming predictions and verifying explanations for behaviour (Berger & Calabrese, 1975).

Thus, the basic premise of Uncertainty Reduction Theory, if one applies the principles to the various company stakeholders, is that it attempts to reduce uncertainty and to increase predictability about each party's behaviour. Gudykunst (1985) emphasised that the ability to verify the other's behaviour alleviates anxiety and vulnerability brought about by high uncertainty. This line of reasoning is based on the argument that if the parties lack confidence in their ability to predict the other's behaviour, feelings of vulnerability will exist.

This suggests that uncertainty can only be reduced by information shared, also that knowledge as to the condition of this information will affect the (un)certainty level. To tie this in with predictability, Kellermann and Reynolds (1990) conducted a series of experiments on uncertainty provoking situations, and found that when the target's behaviour became more deviant, the level of uncertainty increased. Therefore, it can be assumed that when the board reaches a certain level of predictability regarding the quality of information found in the company's financial statements, uncertainty should reduce.

To continue with this line of thought, if others positively confirm one's predictability and expectations, such as auditors that provide independent and objective assurances, an outcome such as trust is likely to be established. The

various company stakeholders would receive independent assurances that their predictions are correct and the board would be shown to be trustworthy in providing sound financial information. Hence, this has a natural corollary to examining the relationship between uncertainty reduction and trust.

3.2.2 Uncertainty Reduction and Trust

In general, trust is defined as a psychological state comprising the intention to accept vulnerability, based upon positive expectations of the intentions or behaviour of another (Rousseau, Sitkin, Burt, & Camerer, 1998). Trust also refers to the notion of the degree one risks: this risk is predicated on the belief that the other party is beneficent and dependable (Johnson-George & Swap, 1982). The notion of trust, according to Mayer et al. (1995), is that trust is the willingness of a trustee *(the recipient of trust or the party to be trusted, i.e. board of directors)* to perform a particular function important to the trustor *(the party that trusts the target party or the trusting party, i.e. investors).*

If no uncertainty exists between two parties, it indicates that no risk or threat will be found in future interaction between the parties (Pearce, 1974). A perfect world does not exist and nor does perfect competition, it is therefore impossible to have absolute uncertainty free interaction *(in other words, a degree of uncertainty always exists).* Both the board of directors and the various company stakeholders should consider this. If one party perceives high uncertainty toward the other party, they feel vulnerable. When the perceived vulnerability is high, no basis for the development of trust will be established (Pearce, 1974). To prevent generating a vulnerable position (as with uncertainty), the trustor should have some confidence in the predication of the trustee's behaviour.

Without a certain degree of predictability, a party has no basic assumption of how the other party will or will not utilise their trusting behaviour (Pearce, 1974). When one party is able to predict, to a degree, the other party's future actions, this leads to a decrease in one's perceived vulnerability (risk is perceived to be reduced). Therefore, uncertainty reduction is a necessary condition for the

development of trust. One party's predictability about the other party should be increased, thus reducing uncertainty via communicating (producing financial statements for the various stakeholders) with each other. As a result, and based upon prior experience, when uncertainty is reduced, perceived predictability should increase and vulnerability will minimise (Flowerday & Von Solms, 2006).

3.3 THE THEORY OF TRUST

Without choking on the plethora of academic, theoretical and even debatable realms of trust, a few points will be covered that address the relevant trust issues pertaining to this study. Trust should not be left in the domain of philosophers, sociologists, and psychologists, but also needs to be addressed by all attempting to practise good corporate governance. Can there be any doubt that fairness, accountability, responsibility, and transparency (King II Report, 2002) are components that contribute to the building and safeguarding of trust?

Trust is not something that simply happens. It is fragile and not easily measured or identified (Handfield & Nichols, 2002). Neither is it an easy concept to define accurately as there are different views and opinions of trust. If trust is defined too narrowly, it may not cover the topic holistically enough. Conversely, if trust is defined too broadly, it becomes an excuse for a host of problems.

Figure 3.1 is a proposed model of trust of one party for another, which highlights the elements of trustworthiness by Mayer et al. (1995). This model illustrates that the level of trust and the level of perceived risk in a situation will have an influence on risk-taking in a relationship. The facets that affect the risk taking in a relationship according to this model are influenced by: the *Trustor*, the *Trustee* and *Perceived Risk*.

The trustor will be influenced by their own propensity to trust another party. The trustor is said to be influenced by how much trust one has for a trustee prior to

information on that particular party being available. Propensity will differ in a party's inherent willingness to trust others (Mayer, et al., 1995).

The Trustee is said to be trustworthy if they demonstrate *Ability*, *Benevolence* and *Integrity*. Mayer, et al. (1995) stress that these characteristics of the trustee, will lead to the trustee being more or less trusted depending on their actions. These characteristics are important if researchers are to understand why some parties are more trusted than others.

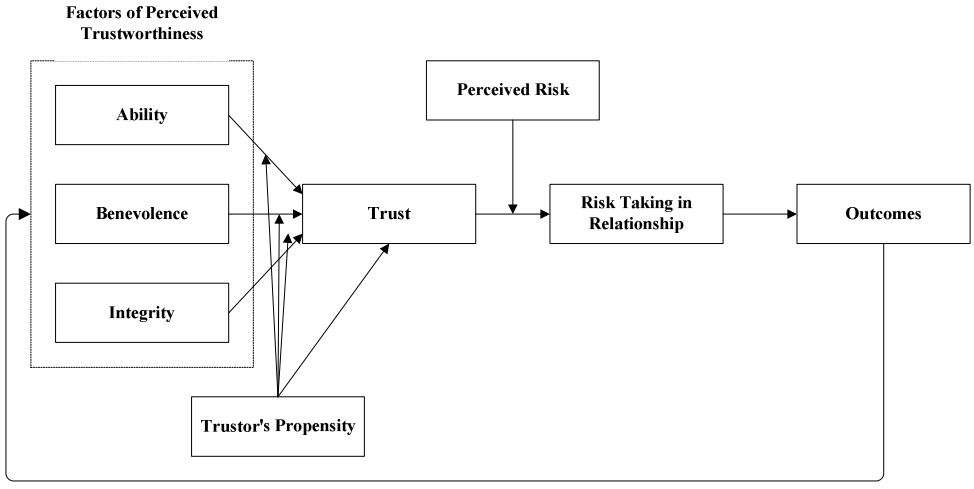

Figure 3.1: Proposed Model of Trust (Mayer et al., 1995)

Once *Trust* has been established, between the trustor and trustee, *Risk Taking in a Relationship* will be influenced by the *Perceived Risks*. To emphasise this important point: *"trust will increase the likelihood of risk taking behaviour"* (Mayer, et. al., 1995, p.726), risk taking behaviour being the *"behavioural manifestation of trust"*. Whether or not a specific risk will be taken by the trustor is influenced both by the amount of trust for the trustee and by the perception of risk inherent in the behaviour. The *Outcomes* (or consequences) of risk taking in a relationship will lead to the updating of prior perceptions of the trustee's ability, benevolence and integrity.

3.3.1 Trustworthiness

The model or a conceptual view of trust proposed by Mayer et al. (1995) will be applied to the board of directors and the various company stakeholders. In this model, the three elements that help to create and define a trustworthy party are discussed. These elements are: *Integrity, Benevolence* and *Ability*. This perception of trust can be applied to corporate governance in the following way:

- **Integrity**-based trust refers to whether the directors are honest and fair and not *"fudging the numbers"* (Fleckenstein, 2005). Some scholars in their research have used the words *predictability* or *reliability* in place of integrity (Ratnasingham & Kumar, 2000; Mishra, 1996). Uncertainty Reduction Theory uses the word, *predictability*.
- **Benevolence**-based trust implies that the directors would be loyal and keep the best interests of the various company stakeholders at heart and not seek to be self-serving and opportunistic. Some scholars have used the words *goodwill* or *openness* in place of benevolence (Ratnasingham & Kumar, 2000; Mishra, 1996).
- **Ability**-based trust relates to the director's *skill level,* for example, their technical competence and understanding of information systems and security. Some scholars favour the word *competence* rather than *ability*, however, very little difference is found in the meanings of these two words (Abrams, Cross, Lesser & Levin, 2003; Ratnasingham & Kumar, 2000; Mishra, 1996).

Perceived trustworthiness requires honesty and integrity. These are attributes that a party needs to demonstrate so that when opportunities to *cheat* arise, they will be turned down. As stated by Mayer et al. (1995), *"… if the trustee had something to gain by lying, he or she would be seen as less trustworthy"*. Conversely, the more perceived benevolence and integrity found in a party, the more likely it will be to predict a favourable future outcome for a relationship with that party (Larzelere & Huston, 1980).

A party's trusting behaviour is seen to be active if they are prepared to voluntarily put themselves in a vulnerable situation in which the other party might actually cause them harm. In perceived trust, vulnerability is minimal and limited, but trusting behaviour involves the voluntary action of making oneself vulnerable to the decisions of others (Pearce, 1974; Rousseau, et al., 1998). Therefore, behavioural trust requires an active process of putting oneself in a risky position. Hence, trusting behaviour involves the components of uncertainty and vulnerability, and they imply that one might lose by trusting the other (Pearce, 1974). This is the case with investors trusting the board of directors to make decisions that are in the investor's interests.

3.3.2 Trust, Risk and Behaviour

Besides behavioural trust, which is an active process of putting oneself in a risky position, there is the notion that perceived trust and perceived risk will influence how one will behave. Gefen, Rao and Tractinsky (2002) contend that perceived risk and trust will affect behaviour and this varies at different stages of a relationship. Risk is dominant in the early stages of a relationship and trust, in long-term relationships.

A cause and effect relationship is applicable when considering the outcomes of decisions, as discussed in Chapter Two. Once again, this principle is relevant when one considers the cause and effect relationship between *'trust and risk',* which has an effect on *behaviour.* This should not be overlooked when addressing the research problem of this project. This concept of trust is important because in order to restore trust, the perceived risks by the various company stakeholders, especially investors, need to be accommodated to avoid a competitive course of behaviour.

Figure 3.2 is a simple illustration of the trust, risk and behaviour concept. Gefen et al. (2002), from their research, have found that the risk perception is more than a mere *"moderating influence"* affecting behaviour (as illustrated in Figure 3.1 by Mayer et al., 1995). They claim that the perceived risk *"mediates"* the effect trust has on behaviour. This has proved to be the case between the board of directors and the owners/investors of a company as illustrated in Chapter Two.

Figure 3.2: Risk Perception Mediates the Effect of Trust on Behaviour
(Gefen et al., 2002)

3.3.3 Game Theory and Trust

Economists and mathematicians have used game theory in their study of trust and behaviour. Various formal models have been proposed over the years since Von Neumann and Morgenstern (1964) first introduced game theory in 1944. These formal trust models based on game theory consider how players discover trust and can quantify how trust or mistrust can occur (Kimbrough, 2005; Murphy, 1991). For the purpose of this study, the principles of two games will be discussed and the mathematical route will not be pursued.

Game theory involves the behaviour of rational decision makers (players), whose decisions affect each other. These players could be the company investors and managers, or any of the company stakeholders that may have conflicting interests. As emphasised (Hayes, 2005; Murphy, 1991), a crucial principle of game theory involves the amount of information known about each other by the various players. What the various players know about each other will determine their behaviour. Also to be noted are the *'rules'* of the game (codes, regulations, policies, etc. that the company needs to comply with).

A classic example of game theory is known as the Prisoner's Dilemma. There are two prisoners in separate cells, faced with the dilemma of whether or not to be police informants. Without further communication, the two players need to trust each other to have integrity and to be benevolent. The following are possible outcomes to this scenario.

If neither become informants and defect, the police have insufficient or only circumstantial evidence to convict them and therefore both players receive light sentences. If trust is lacking and both turn and become informants for the police, through their defection both players receive heavy sentences. If one player defects and becomes a police informant, that player is set free and the player that did not defect is convicted and receives a very heavy sentence due to the testimony of the player who defected. The dilemma of the scenario highlights the issue of trusting the other player without continuous communication. In the case of this research project, the communication is the financial information of the company. Is the financial information a *fair representation* of the financial position of the company or not? Are the *threats* to the accounting information systems adequately addressed?

As observed by Khare and Rifkin (1998), if the police tell the prisoners (players) that the interrogation is ongoing and without a foreseeable end, a pattern emerges and cooperation can become stable. This is the discovery of trust as the players learn to trust each other over time and the risk element is reduced. If one applies this model of trust to corporate governance it can be assumed that, over time, trust will be established between the various stakeholders, including the CEO, the board of directors and investors.

Axelrod (1997) suggests that, with time, a pattern of cooperative behaviour develops trust as in game theory. However, one could trust the director's ability (technical and information security capabilities), but not necessarily their integrity because they may act opportunistically. This highlights that trust is

more specific than *'I trust the board of directors'*. One should clarify what it is that I trust the board of directors to do.

To explain this concept another way, an everyday example proposed by Flowerday and Von Solms (2006) will be used. Note that trust is not transitive and is rather domain specific (Zand, 1972). Example: one might entrust a colleague with $100 loan, but not entrust the same resource to that colleague's friend whom you do not know. Trust therefore weakens as it goes through intermediaries. Furthermore, to emphasise a related aspect, one might trust a colleague by loaning them $100, but not allow access to your bank account to withdraw the $100 themselves. The second example highlights the domain specificity of trust. One does not blindly trust, but one trusts a party in a specific area or domain.

To continue with the prisoner's dilemma, the interests of the players are generally in conflict. The dilemma comes from the fact that if both individuals choose the high-risk option (both remain silent), both individuals receive positive outcomes, which is the ideal situation. If both choose the low-risk option (both confess), both receive negative outcomes. However, if one chooses the high-risk option and the other chooses the low, the former receives a maximised positive outcome and the latter a maximised negative outcome.

The cases of opportunistic behaviour, discussed in Chapter Two, by the CEO and/or members of the board of directors have highlighted this situation and it has been to the detriment of the investors. The investors chose the high-risk option and remained committed to the relationship and lost financially (share prices went down). Many members of the board of directors *'defected'*, choosing the low-risk option and short-term financial gains by selling their shares or overly stating the company profits so that they could receive their bonuses. Moreover, this illustrates that the investors lacked information privy to the directors. The opportunity arose to *'cheat'* and many of the directors took advantage of the opportunity.

Kydd (2005, p.10) sheds a different light on the Prisoner's Dilemma by pointing out that, strictly speaking there is no uncertainty about motivations, or behaviour and that the dominant strategy is to defect. As a result, uncertainty is smuggled in through the back door. He continues to emphasise that *"…trust is fundamentally concerned with this kind of uncertainty"*.

Kydd's research discusses trust and mistrust, and claims that there is no uncertainty in the prisoner's dilemma about whether the other side prefers to sustain the relationship. He questions whether future payoffs are valued highly enough to make sustained cooperation worthwhile, or if they are not, the parties will defect. He states that trust is therefore perfect or nonexistent. To model trust in the prisoner's dilemma one must introduce some uncertainty, either about preferences or about how much the parties value future interactions (Kydd, 2005, p.11). Applying Kydd's argument to the various company stakeholders illustrates that there needs to be a *'win win'* situation for all. The information one party has, also needs to be available to the other parties. Conflicts of interest need to be avoided so that the benefits of opportunistic behaviour are minimised.

Another game theory game, the *Stag Hunt*, which is in harmony with this research project's proposed solution, is less well known than the Prisoner's Dilemma. Nevertheless, the Stag Hunt game is also known as the *Assurance Game.* Assurance, being core to this study, heightens the importance of understanding the principles of this game. An important point is if one side thinks the other will cooperate, they also prefer to cooperate. This means that the players with the Assurance Game preferences are trustworthy. Kydd (2005, p.7) states: *"They prefer to reciprocate cooperation rather than exploit it"*. This conveys that it makes sense to reciprocate whatever you expect the other party to do, trust or suspicion/mistrust.

The Stag Hunt *(assurance game)* is about two hunters that can either jointly hunt a stag (an adult deer/buck, a rather large meal) or individually hunt a rabbit

(tasty, but substantially less filling). Hunting a stag is quite challenging and requires mutual cooperation. If either hunter hunts a stag alone, the chance of success is minimal. Hunting stag is most beneficial for the group, but requires a great deal of trust among its members. Each player benefits most if both hunt stag, thus, by hunting stag together both players trust the counter-player to do likewise. Conversely, a player hunting rabbit lacks trust in the counter-player. Deciding not to risk the worst outcome (not getting the stag) is to decide not to trust the other player. Conversely, *"if trust exists then risk can be taken"* (Kimbrough, 2005).

Cooperation is possible between trustworthy parties who know each other to be trustworthy. This can be likened to the CEO, the board of directors, and the investors. They need independent and objective assurances that the other party is trustworthy and the information shared is not compromised information. In the Prisoner's Dilemma, cooperation can be sustainable only if the players care enough about future payoffs because they will fear that attempts to exploit the other party will be met with retaliation (Axelrod, 1984). In the Assurance Game (Stag Hunt), the level of trust one party has for the other party, depends on the assessed probability the other party is trustworthy (Kydd, 2005).

Kydd (2005, p.9) adds that the minimum trust threshold will depend on the party's own tolerance for the risk of exploitation by the other side. To consider the situation of the CEO, directors and the investors, cooperation needs to be the overwhelming option to avoid cheating and mistrust. This leads back to the elements of the trustworthiness model proposed by Mayer et al. (1995) that integrity, benevolence and ability are needed to demonstrate one's trustworthiness. The best option is clearly to demonstrate trustworthiness and hunt the stag together, as this maximises the return on effort and becomes a *'win win'* situation for both parties.

The stakeholders should have this *'win win'* goal and develop cooperative behaviour between them. The development of positive uncertainty reduction

should be the basis for engaging in cooperative behaviour. When a piece of positive information (financial statements with assurances) about the company is presented, the uncertainty will be reduced, and as a result, the chance of engaging in cooperative behaviour will be increased. In contrast, where higher uncertainty levels exist between parties, or a piece of information confirms negative predictions, then the competitive course of action will more than likely be adopted.

In a cooperative situation, both participants feel that they are perceived as benevolent. Therefore, in this case they can willingly place themselves in vulnerable positions (behavioural trust). Under this condition, the various parties are likely to establish or perceive a relationship of mutual trust. This again highlights the point that the stakeholders need assurances to trust the information found within the financial statements (validation by auditors). This emphasises the importance of information security and that it should safeguard the *accuracy* (fraud) and *reliability* (confidentiality, integrity and availability) of information.

3.4 RISK, SECURITY AND ASSURANCES

As intimated, it is vital that positive predictability needs to occur for trust to increase between the various parties (stakeholders). Therefore, one should ensure that through various security mechanisms, the information found within the financial statements is not compromised as this would have a negative effect. The knowledge, via independent and objective assurances, that information security is adequate and the risks contained, assists in building confidence.

3.4.1 The Dark-side of Trust: Risk

Queen Elizabeth 1st in her address to Parliament in 1586 concluded with: *"In trust I have found treason"* (Partington, 1996). At what stage of a relationship is one relying on trust to the point that one is overly exposed to risk? In perfect competition, Humphrey and Schmitz (1998) contend that *"risk is ruled out by the assumptions of perfect information and candid rationality"*. However, they

emphasise that, in today's world the issue of trust exists because transactions involve risk, as we do not have perfect competition.

Noorderhaven (1996) observes that, in the context of a transaction relationship, if adequate security safeguards are in place for a transaction to go ahead, then it is not a trust transaction. However, if the actual information security safeguards and controls in place are less than adequate, a trust-based relationship is assumed as the existence of trust is inferred. The assurances provided by the auditors should include whether the safeguards and controls are adequate or not and report (validation) on the condition of the information. This would allow a party (trustor) to know how exposed they are when they consider if the other party (trustee) is trustworthy or not.

To expand on this, risk is present in a situation where the possible damage may be greater than the possible return (Luhmann, 1988). Therefore, as stated (Rousseau, et al., 1998), *"risk creates opportunity for trust"*. This is in harmony with Gefen et al. (2002) and game theory (Hayes, 2005; Axelrod, 1997) who postulate that trust can *grow* and *evolve* over time. In addition, it is acknowledged that trust is a neglected resource for economic development and that stable, clear and enforceable rules help to promote economic development (Humphrey & Schmitz, 1998). These rules limit uncertainty and hence increase the likelihood of trust.

It reinforces the premise that trust can decrease uncertainty about the future and is a requirement for continuing relationships where parties have opportunities to act opportunistically (Limerick & Cunnington, 1993). This is in agreement with the theory that trust affects the trustor's risk taking behaviour (Mayer et al., 1995). To summarise, *"if the level of trust surpasses the perceived risk one would engage in the relationship"* (Flowerday & Von Solms, 2006).

3.4.2 Trust and Security

As highlighted, trust is the positive view of risk exposure as *"trust is risk"* (Camp, 2000, p.2). Camp (2002, p.16) further advocates that both *"technical competence"* and *"good intent"* are required to ensure security. She emphasises that efforts at securing information systems should involve not only attention to networks, protocols, machines and policies, but also a thorough understanding of how social agents (individuals and parties) participate in, and contribute to trust. One can lose sight of the fact that conventional security technology, if implemented perfectly, still does not equate to trust (Khare & Rifkin, 1998).

An example to illustrate the point that Khare and Rifkin make is if one were to sign a legally binding contract (e.g. lease agreement) it makes the transaction contractually sound and secure. However, trust has not been established. In other words, even if the company's system of internal controls is adequate it may assist in safeguarding trust, but it alone does not build trust.

Camp (2002) stresses that, *"security is not a separable element of trust"*. This statement is collaborated by Ratnasingham and Kumar (2000) as they contend that both trust and security-based mechanisms are classified as safeguard protective measures. They claim that these protected measures provide benefits, such as efficiency and quality to business. Additionally, these provide technological, organisational and relationship benefits to the various company stakeholders.

This introduces the concept that conducting business electronically, within the information economy, raises information security from a technical issue to a business issue (Dang van Mien & Green-Armytage, 2002). In fact, information security has become a corporate governance challenge and therefore requires all levels within the company to be conscious of the vulnerabilities and risks facing the company (Conner & Coviello, 2004; Conner, et al., 2004).

This accentuates the fact that although it may be desirable, 100% security is not feasible and it is commonly accepted that not all risk can be eliminated (Greenstein & Vasarhelyi, 2002). This residual or inherent control risk is based on the notion that additional investments in controls or safeguards will not eliminate this risk. This means that the various company stakeholders are forced into a trust-based relationship, bearing the associated risks as they pursue the benefits of an information economy. Since risk exists in transactions, it is very important that investors concern themselves with the trustworthiness of the other party (Ring & Van de Ven, 1992). So accordingly, even when signing a secure contract (e.g. lease agreement) there is still inherent or control risk involved.

Figure 3.3 (Flowerday & Von Solms, 2006) illustrates how trust and controls work together in securing a transaction or a business process. Triangle A, B, D is the *Control* area and triangle A, D, C is the *Trust* area. The line E, F is a hypothetical positioning of the company's Risk Appetite. The area of the rectangle A, B, D, C is the business process area or transaction area. When one views the Risk Appetite line (E to F) one will note that the white area is protected by controls and the dark area is the *'risk'* exposure or the area *protected/secured by trust*. Depending on how much the parties *trust* each other will affect the positioning of the Risk Appetite line. This figure will be discussed in more detail in Chapter Four.

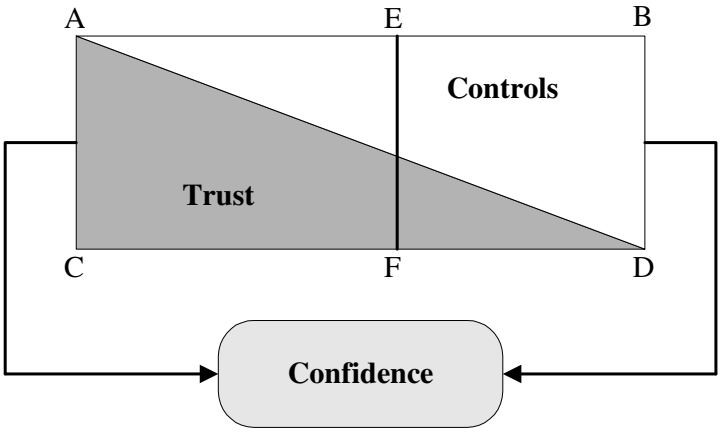

Figure 3.3: The Relationship between Trust, Controls and Confidence
(Flowerday & Von Solms, 2006)

The confidence that the various company stakeholders have in their relationship is determined by two factors: one being the level of trust and the other the perception of how adequate or inadequate the controls are that govern the conditions of the arrangement (Cox & Marriott, 2003). To achieve a favourable relationship between the stakeholders, one has to find the right balance between trust and control. In addition, one has to find the optimal balance between the costs of the controls versus the desired level of trust. The cost of controls will also help determine where the Risk Appetite line is to be positioned.

The control elements of information security will be discussed in more detail in Chapter Four where it is argued that both trust and control are required to have confidence. However, to summarise: absolute trust and absolute control are two opposing extremities of approach for attaining confidence (personal communication, Alex Todd, August 2005). The solution is somewhere in the middle ground between trust and control, as shown in Figure 3.3. There are those that argue the company should position itself on the trust side in an effort to reduce transaction costs (Fukuyama, 1996, p.27; Todd, 2005). However, practicalities and realism are *forces* that pull the solutions into the control end of the spectrum.

As the investors own the company, which is controlled and managed under the board's supervision, the 'other party' is considered to be the board of directors and executive management *(agency theory)*. It is widely accepted that reduced risk and increased trust are both likely to increase the likelihood of engaging in a relationship (Gefen et al., 2002). Additionally, DeMaio (2001) champions that one should try to build business environments based on each party's willingness and ability to continuously demonstrate to the other's satisfaction that all dealings are honest, open, and that the rules are followed. He states, *"e-Trust is all about mutual assurance"*.

3.4.3 Mutual Assurance

Mutual assurances help to build confidence between the various company stakeholders in a similar manner to the hunters in the Stag Hunt *(assurance)* game. In the same manner, VeriSign can provide confidence that your email is encrypted and untainted because of its independence. Therefore, it follows in principle that auditors verify a company's financial statements and provide assurances as to the condition of the information - *validation*. The only difference is that VeriSign and the Stag Hunt game provide the assurance in *real-time*, something the auditing profession needs to address. This too will be discussed in more depth later in this thesis.

Mutual assurance should exist between stakeholders, reassuring each other that the risks are mitigated to an acceptable level and that the degree of (un)certainty is appropriate. The adage of *trust but verify* should exist as the various stakeholders demonstrate to each other, via objective and independent audits, that the agreed upon best practices are maintained.

It has been found while conducting this literature survey that many different views on trust, assurance, security, and the auditor's role exist. To make a general assumption and to clarify the line of reasoning for this study, the security practitioners have the role of implementing the system of controls. The board of directors, and management, seek assurances from the auditors that their system

of controls in place is adequate. The auditor is there to give an independent and objective view and verify the effectiveness and sufficiency of the controls. In other words the auditors provide a *'true'* picture of the information, and the data that make up this information, within the financial statements. The auditors provide the truth. The assurances, if positive, add to uncertainty reduction and therefore increase mutual trust.

3.5 A TRUST STRATEGY

Strategy, by its nature, concerns itself with the future as one strategises in an attempt to gain a competitive advantage. Companies today operate in an uncertain world where the markets have become increasingly more competitive. The Turnbull Report (1999) emphasises that taking risks is what companies do. It is the justification for profit and therefore the identification and assessing of risks are required, so that the risks are appropriately managed.

A company should craft a strategy considering their relationship with their various stakeholders. An important aspect of this strategy is managing the uncertainty of future events, i.e. managing and containing the risks to an acceptable level. The board of directors should consciously attempt to *build* and *safeguard* trust between them and their investors so as to have a favourable relationship.

Table 3.1 is a summary of Todd's work (2005) where he researched trust in the technical arena, specifically focusing on e-commerce. He divided trust into two domains and had three subsections in each domain. Todd has based his work on Gerck (2002), who is an academic and Internet security expert. Gerck appears to have originally divided trust into these two domains, *establishing* and *ensuring* trust. Furthermore, Gerck focused on trust refinement and risk refinement as a means of reducing uncertainty.

Table 3.1: Trust Establishing and Ensuring Services (Todd, 2005)

Trust Establishing Services *"trust refinement & establish trust (Gerck, 2002)"*	**Trust Ensuring Services** *"risk refinement & ensure trust (Gerck, 2002)"*
Witness Related Services	Governance
Expert/Authority Services	Risk/Opportunity Sharing
Introduction Services	Controls

For the purpose and focus of this research project, the domains have been renamed to *Building* and *Safeguarding* trust and the subsections have been modified accordingly. From the study of the concept of trust it appears that one builds trust over time and then one needs to safeguard trust due to its fragile nature. The following points in Table 3.2 (Flowerday & Von Solms, 2006) should be taken into account when one considers building and/or safeguarding trust and creating a company trust strategy.

Table 3.2: Building and Safeguarding Trust (Flowerday & Von Solms, 2006)

Building Trust	**Safeguarding Trust**
Benevolence/Openness	Risk Management
Ability/Competence	Security Safeguards and Controls
Integrity/Predictability	Compliance
Constant Communication	Recourse Mechanisms
Ethics	Governance
Assurances	'Assurances'

To revisit the Prisoner's Dilemma, (personal communication, Alex Todd, July 2005) as discussed, it also teaches us that there is an incentive to seek short-term competitive advantage by being dishonourable. However, this is only likely to work under limited circumstances, such as:

- The directors are able to hide their opportunistic behaviour and not suffer the negative consequences.
- The directors will no longer need to satisfy their investors (closing down, directors moving on) therefore the value of being dishonourable exceeds the negative consequences.

A company, in their strategy, should attempt to mitigate their risks to an acceptable level by reducing the value of opportunistic behaviour from occurring. Moreover, information security audits should be preformed to assure that the technical side of security is adequate as security helps to safeguard trust. Finally, assurances help to establish trust in the level of confidence placed in the information. The assurances establish a more accurate level *(the truth)* of trust as to the condition of security safeguards and controls. To refer back to the Stag Hunt/Assurance Game, it is the assurances provided by one hunter to the other that keep them *'confident'* that both parties are committed to the hunt. If not, insecurities 'creep' in and alternatively a hunter may decide to hunt a rabbit and the Stag Hunt collapses. Establishing trust sets a level of confidence.

Hence, the directors need to consciously *build* stakeholder trust by demonstrating trustworthiness by providing *reliable* and *accurate* information. In addition they need to communicate regularly with the various stakeholders and ensure that objective assurances are provided with the information when the information becomes available, not months later. In their effort to *safeguard* trust, good governance, including sound risk management practises and information security, must be ensured.

3.6 CONCLUSION

Trust and information sharing between the various company stakeholders has taken place since formal commerce began. The information's integrity is of utmost importance, especially the information found within financial statements. This information needs to be trusted. However, the various stakeholders have their own goals and motivations in addition to the shared goals. Conflicts of interest arise and each party is vulnerable. Each also needs to trust the other to have *integrity*, *benevolence,* and *ability* or in other words to be trustworthy. Companies should have a trust strategy to guide them in building and safeguarding trust; with independent and objective assurances being part of this strategy.

To have a positive outcome, trust needs to increase and uncertainty needs to be reduced to an acceptable level. This could be through assurances provided by auditors *validating* the *reliability* and *accuracy* of the information (the auditors report on the system of internal controls and the information within financial statements) or through evolving relationships (as discussed in game theory). To avoid unfavourable behaviour, uncertainty needs to be contained and the level of trust needs to surpass the perceived risks (Flowerday & Von Solms, 2006). This will ensure that a relationship will flourish. Within a competitive society, the various company stakeholders cannot enter partnerships with blind trust, believing that everyone will do the right thing (Bavoso, 2002). Incidents like the Enron, WorldCom, Tyco, and Parmalat debacles are fresh and painful reminders.

The development of cooperative behaviour and mutual trust should be the goal of all company stakeholders. One cannot escape that trust affects confidence and is the reason for acceptance of a degree of insecurity (as shown in Fig. 3.3). To conclude with the point Camp (2002) makes that both *"technical competence"* and *"good intent"* is required to ensure security, it is important to trust both the information systems infrastructure and the data that make up the information in the financial statements. However, one also needs to trust the human element not

to manipulate and compromise the information for self gain, but to demonstrate trustworthiness.

Therefore, *"confidence in information security management requires trust and trust requires information security to help safeguard it"* (Flowerday & Von Solms, 2006, p.97). This leads to the next chapter on internal controls, which will assist in safeguarding trust and mitigating risk.

Chapter 4

INTERNAL CONTROLS

"Better be despised for too anxious apprehensions, than ruined by too confident security."

- Edmund Burke, (statesman and philosopher, 1729 – 1797)

4.1 INTRODUCTION

Risk is intrinsic to governance and to address one of these areas is to simultaneously affect the other. Additionally, the concepts of trust and risk are significant variables. Risk being, ubiquitous in nature, needs to be addressed thoroughly. Shaw (2003, p.147) succinctly stated: *"One may not manage risk, but one can manage for risk"*. As discussed in Chapter Three this statement can also be applied to trust.

The need to manage *for* risk accentuates the importance for an enterprise risk management framework such as COSO-ERM (2004). This framework assists in guiding the decision-making process so as to not expose the company to undue risk in its attempt to provide value for the company stakeholders. As emphasised, risk management is core to corporate governance and risk management includes an information security framework (Conner & Coviello, 2004). To have an effective information security framework a system of internal controls, including IT controls, is required in order to address IT risk. Part of this control framework should include a monitoring system of these controls to assess their effectiveness and efficiency.

The type of risk being considered is not speculative financial risk, strategic risk or reputational risk, but rather *operational risk*, more specifically *IT Risk*. The nature of IT Risk and information assets is that they are woven throughout the fabric of the company and are embedded in the business processes.

This chapter argues why a sound system of internal controls is required to ensure information integrity. Knowing that the company has an effective enterprise risk management framework in place, including a system of internal controls, allows the decision-makers and users of information, confidence when basing their decisions on the company's financial information.

This chapter first reviews the argument that both controls and trust are required to achieve confidence, followed by today's current risk management practices. The chapter concludes with a detailed discussion on internal controls, specifically IT controls, and how this system of controls can effectively manage operational risk and uncertainty.

4.2 CONTROLS AND TRUST

Figure 4.1 is the same as figure 3.3; however, the *Controls* side is highlighted in place of the Trust side. As noted in Chapter Three, the right balance between trust and controls need to be found in order to achieve confidence. There are those who argue that a Trust model should be the preferred management approach in an attempt to manage risk. The trust 'advocates' claim that the trust models enable reduced transactions costs, increased flexibility and collaboration (Fukuyama, 1996, p.27; Hagel & Seely Brown, 2002; Todd, 2005).

Conversely there is a 'large school' suggesting that management should *'batten down the hatches'* in an attempt to control the activities and business processes of the company (Allen, 2005; Becht, et al., 2002; Boritz, 2005; Conner, & Coviello, 2004; CobiT, 2005; COSO-ERM, 2004; COSO-ICF, 1992; Flowerday & Von Solms, 2005a; Greenstein & Vasarhelyi, 2001; GTAG1, 2005;

ISO/IEC17799, 2005; Jordan & Silcock, 2005; Lindberg, 2005; Morrison, 2004; Peltier, 2001; Shaw, 2003). Whichever side is supported, both need each other to achieve confidence, as absolutes in either case are not achievable. Trust needs controls to safeguard it and the controls need to be trusted that they are functioning adequately. The process of reducing uncertainty and establishing an acceptable confidence level needs both trust and controls.

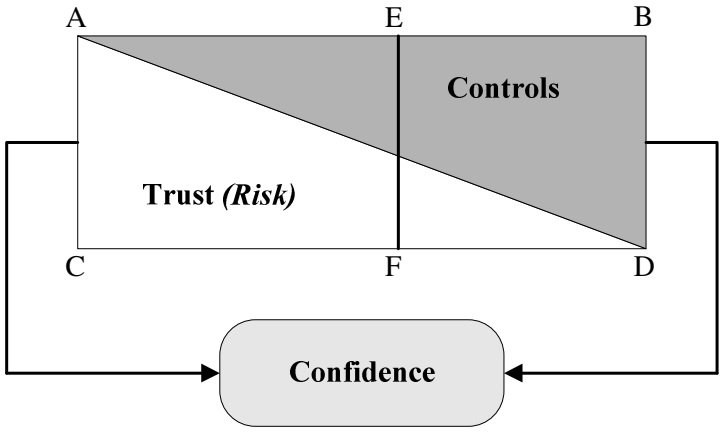

Figure 4.1: The Relationship between Controls, Trust and Confidence
(Flowerday and Von Solms, 2006)

But, with escalating competition, increasing risk and growing uncertainty are conditions that unsurprisingly favour the 'control school'. An important driver behind the motivation for controls is to shield and safeguard predictability, company stability and reduce uncertainty. However, Hagel and Seely Brown (2002) contend *"the control mindset cannot cope"* because *"control requires the ability to dictate all activities"*. They assert that companies are becoming more *interdependent* and require increased flexibility and collaboration. They maintain this is contrary to the 'control school' principles.

Nonetheless, *in theory*, the loosely coupled business activities proposed in the trust models (Hagel & Seely Brown, 2002; Todd, 2005) do appear to be more flexible and do appear to encourage collaboration. Moreover, it is agreed that a

thorough system of controls is costly, adding to the company's financial overhead and therefore increases transaction costs (Fukuyama, 1996).

Nevertheless, with too few controls the company is exposed to increased risks and compliance issues. Chapter Two noted the corporate governance failures when trust was relied on and controls relaxed. For one to effectively manage the company's activities, *even if rigid*, an effective system of controls is required. This control-based approach will enable managers to intervene at any time to clarify their expectations or rectify a situation, provided an effective real-time monitoring system is in place.

Trust is required to help establish confidence and *in theory,* is an effective way of mitigating risk. However, the preferred option is a system of controls. One of the reasons is that in order to establish trust to the degree that it works effectively enough to mitigate risk, requires a great deal of time, based upon prior experience between the parties. Within the fast moving corporate environment of today, the luxury of time is often not available. Therefore, this leads to the next section which illustrates today's preferred way of risk management.

4.3 RISK MANAGEMENT

Risk, in general, can broadly be defined as the possibility of something adverse happening. A more specific definition by the ISO/IEC 13335-3 Technical Report (1998) states; *"the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets"*. It is noted that risk management involves addressing the risks in such a way that they are brought under control, thus resulting in minimising the possible damage to an information system or asset (Gerber & Von Solms; 2005).

Therefore, one needs to understand where the potential risks may occur then decide if these risks will be accepted or controlled using countermeasures. As emphasised by COSO-ERM (2004), the company needs to consider *all* risks that

they may be exposed to and that may cause harm. When investigating risk management a myriad of methodologies were found. The main objectives of the risk management process are to *Identify*, *Evaluate* (this will be influenced by the company's risk appetite), *Manage* (or control) and to provide *Assurance* that your risk strategy is working.

Management needs to decide how to apply their resources to manage the company's risk and the auditors should be in agreement (Hunton et al., 2004). The risk management process attempts to balance the risks against the needs of the company (Peltier, 2001). The goal should be to mitigate the risk to an *acceptable* level as no company can afford the resources to mitigate risk to a zero level (Greenstein & Vasarhelyi, 2001; ISO/IEC Technical Report, 1998; Jordan & Silcock, 2005; Marchany, 2002; NIST 800-53 Publication, 2005; Peltier, 2001).

Managing information risks and practising due care are essential to any company (Horton et al., 2000). However, today, risk management takes on a new emphasis with regulations such as the Sarbanes-Oxley Act (2002) and the Basel II Accord (2004), emphasising internal controls, transparency and accountability. These regulations *'go further'* than before, requiring transparency in the operational processes and the data that make up financial statements.

4.3.1 Operational Risk

Management has always practised risk management in their operational decision making process. However, their approach to risk and the degree of success has varied. The day-to-day operations within the company and its business processes determine the successes or failure of achieving incremental progress towards the company's defined goals and objectives. There are also accompanying risks in each operation that could deter progress towards these goals and objectives. The ability to anticipate and manage these risks is critical to maintaining successful ongoing operations. IT risk is classified as a subsection of operational risk (Basel II, 2004).

Defining Operational Risk is not straight forward nor readily agreed upon. Possibly this could explain why the definition is so broad and encompasses so much. However, earlier this decade, a common definition emerged even though some parties have their own modified versions of this definition: "*… the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events"* (Basel II, 2004, pg.120). This definition further includes legal risk, but excludes strategic and reputational risk. It is also pointed out that the loss could be caused as a result of *direct or indirect risk*.

When this definition is contemplated, operational risk management becomes rather holistic and inclusive, highlighting the importance of an effective monitoring system so as to understand the company's operational risk status. The nature and complexity of business processes and company systems can be likened to a human's blood circulatory system. It is ubiquitous in nature and endogenous to the company. Thus, it can be concluded that if not managed properly, in its entirety, the risk to the company could be too high and even fatal. Hence, the current increased focus on operational risk.

4.3.1.1 Basel II Accord (2004)

The Basel II Accord or The New Basel Capital Accord from The Basel Committee on Bank Supervision is constructed around three pillars:

- 1st Pillar covers the calculation of minimum capital requirements for the bank. It requires the bank to consider their Credit Risk, *Operational Risk* and Trading Book Issues. Operational Risk, *of which IT Risk is a subsection*, has been catapulted into the limelight with this accord and a capital charge for the first time is required to 'cover' this risk.
- 2nd Pillar stresses the importance of the Supervisory Review Process and emphasises that the bank's board of directors has a responsibility to ensure that management establishes a system for assessing the various risks. Additionally, one needs to develop a

system to relate risk to the bank's capital level, which *"establishes a method for monitoring compliance with internal policies"* and *"adopts and supports strong internal controls"* (Basel II, 2004, pg.140).

- 3rd Pillar encourages the Market Discipline where the bank is required to provide *disclosure of their risk management practices and processes*, including operational risk.

Within the Basel II Accord, it is acknowledged that approaches to Operational Risk are continuing to evolve. Nevertheless, they are not likely in the near term to attain precision. Meanwhile, they encourage banks to use their own methods for assessing their exposure to operational risk. Many companies are actively attempting to manage and mitigate their risk as they safeguard their assets (especially information assets as highlighted in Chapter Two); yet their efforts represent only a partial reduction in IT Risk (Basel II, 2004). This once again highlights the importance of IT risk management and of information security management.

4.3.1.2 Sarbanes-Oxley Act (2002)

The Sarbanes-Oxley Act, also known as The Public Company Accounting Reform and Investor Protection Act, promotes greater control, transparency and risk management in the financial and accounting arena of companies listed on US stock exchanges, and it was signed into law on the 30 June 2002. The Act aims to *"enhance corporate governance through measures that will strengthen internal checks and balances and, ultimately, strengthen corporate accountability"* (Rector & Davis, 2005).

Some of the sections of the Act have a direct effect on IT Risk. For example, Section 404 *"Management Assessment of Internal Controls"* does not merely require companies to establish and maintain adequate internal controls, but also to assess their effectiveness on an annual basis (as noted in Chapter Two). Today most of the accounting and financial systems used in companies rely on

information systems, in which the *adequacy* of the information security controls are of paramount importance to Section 404. This section in particular has caused a tremendous amount of 'excitement' within the IT auditor community.

As noted in Chapter Two, Section 409 is about *"Real Time Issuer Disclosures"*. This requires that there is a monitoring of *operational processes* or as put by Emery (2004), *"section 409 will demand a dynamic risk management framework to monitor operational risks"* and file material events with the Securities and Exchange Commission within four working days. In Finland, any materiality needs to be filed within *one* working day and so is even more demanding. As stated earlier, IT Risk constitutes a major subsection of operational risk, therefore directly related to risk management and hence corporate governance.

The following sections of this chapter discuss two approaches of assessing and managing risk in more detail. The focus is a business process approach using a system of internal controls addressing *'likelihoods'*.

4.3.2 The *Process* of Risk Management

As established, a risk is an uncertainty about a potential threat that will exploit a particular vulnerability without the company being equipped to manage it (Peltier, 2001). It is the board of director's responsibility to demonstrate that it has dealt comprehensively with the issue of risk management and internal control (Basel II, 2004; King II Report, 2002, pg.79; Sarbanes-Oxley Act, 2002). Risk management is crucial for the sustainability of the company and information security management is crucial for risk management.

The risk management strategy that the board chooses should be in line with the company's risk appetite (King II Report, 2002). Four strategies to managing risk are discussed (Whitman & Mattord, 2003). These are:

Risk avoidance – This is a strategy of avoiding risks altogether instead of having to address the consequences of these risks. This includes a risk control strategy that attempts to prevent the exploitation of vulnerabilities by countermeasures.

Risk transference – This strategy involves transferring the responsibility of the particular risk to another party, for example outsourcing or purchasing insurance.
Risk acceptance – Here the company accepts the potential risk and continues operating the IS/IT system regardless of the risk. This decision is based on the conclusion that the cost of protecting the asset does not justify the security expenditure.
Risk mitigation – This is a control approach to reduce the impact caused by the exploitation of vulnerabilities through planning and preparation. It is the ability to respond quickly, efficiently and effectively to attack. For example this includes an incident response plan, disaster recovery plan and business continuity plan.

When the board ensures that a thorough risk analysis has taken place and adequate risk countermeasures have been put in place, the directors are fulfilling their responsibility and *due diligence* has taken place. The risk management efforts assist the directors in guiding their decisions and thus sustaining the company by avoiding harmful threats.

Nevertheless, the board of directors has the driving need to strive for profitability and the maximisation of shareholder wealth as their overarching corporate goal (Piper, 2002). Chapman (2001) adds; *"Good business is all about risk: business growth cannot occur without introducing new risks, business objectives cannot be achieved without placing assets at risk; and business rivalries cannot be won without 'out-risk-taking' the competition"*. This is in line with the investor principle that risk is usually proportional to gain, i.e. accept the risk if the benefit exceeds the risk.

This appears to be a quandary or dilemma for the directors, maximising shareholder wealth and balancing this with the risks involved. The directors need to use all the tools, techniques and help available to make informed decisions and to carry out their duties and responsibilities with *due-care* (avoidance of negligence). It has been noted during this literature survey that the

commitment to risk management is strong; it is the execution thereof that continues to evolve and remains 'weak'.

The risk management process itself is not new; rather, it has been refined over the years. It has been around in various forms for several centuries, and the insurance industry, followed by the banking industry has helped to develop this field. However, as stated earlier, corporate dependence on information technology has resulted in significant additional threats that lead to risks to which the companies are exposed. A risk assessment model developed within the IT security community, the Common Criteria (2004), illustrated in Figure 4.2, helps to decide if countermeasures *(safeguards/controls)* have the desired impact and are adequate in controlling the risks.

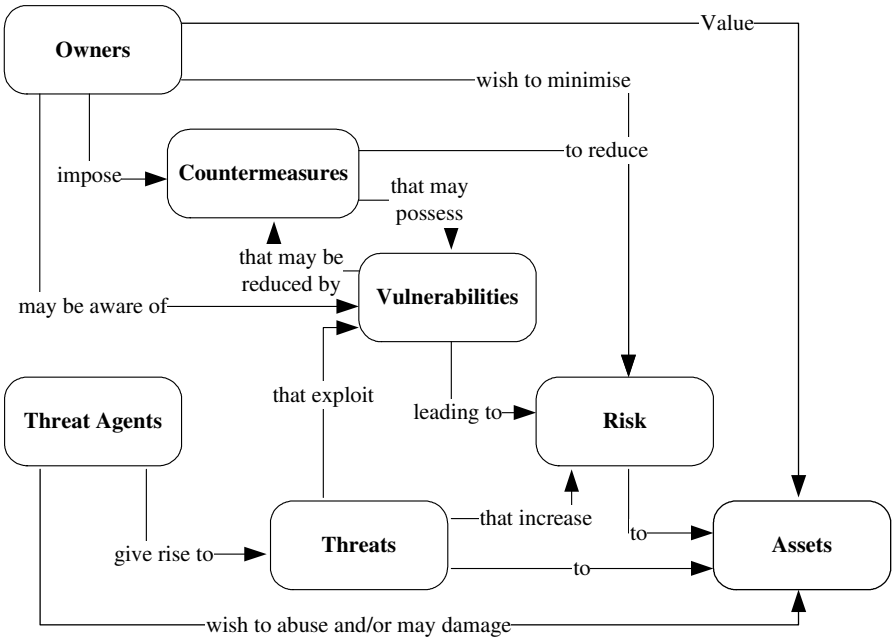

Figure 4.2: Security Concepts and Relationships (Common Criteria, 2004)

The desired level of risk (risk acceptance) is crucial in determining the company's *Risk Appetite* when allowing for countermeasures. Each company has a different risk appetite. The company stakeholder's attitude towards risk,

the company mission statement, the industry the company operates in and their current strategy will all help to determine their risk appetite *(positioning of line E, F in Figure 4.1).* The IT Governance Institute (ITGI, 2003) points out that effective risk management begins with a clear understanding of the company's appetite for risk.

It is stressed that the directors should indicate the level of risk appetite (Applegate & Wills, 1999; COSO-ICF, 1992; Von Solms, 2003). While line managers must, through their 'ownership' of information systems, indicate the importance of the systems and databases to the company (Von Solms, 2003). Additionally, management should be doing the risk assessment, the identification and analysis of the relevant risks to enable them to achieve predetermined objectives (Applegate & Wills, 1999; COSO-ICF, 1992; Von Solms, 2003).

4.3.3 Threats, Vulnerabilities and Probabilities

One approach to risk management is to identify *threats*, associated *vulnerabilities* and the *probabilities* of occurrence. A formula can assist in the decision making process when determining the *cost* of the risk. Firstly, estimated values need to be assigned to the *Likelihood of the Loss (%) (probability)* and *Loss from the Specific Risk ($) (vulnerability).* The expected value of the specific risk is calculated as follows:

$$\textbf{Expected Value of Specific Risk} = \frac{\textbf{Estimated Loss from Specific Risk (\$)}}{\textbf{Likelihood of Loss (\%)}}$$

Theoretically, management should be willing to spend an amount equal to the *Expected Value of the Specific Risk (threat)* to control it (risk avoidance and mitigation), or purchase insurance (risk transference) to offset the loss (Hunton et al., 2004). The problem with this approach is that if one takes this quantitative perspective, at times, extreme numbers are produced that lack legitimacy (Flowerday & Von Solms, 2005a). Consider, for example, the 11th September

2001 World Trade Centre disaster in New York. The following are not actual figures, but merely to illustrate the example.

The probability of the occurrence is approximately one million to one and the loss due to the probability occurring was approximately five billion dollars. The resultant Annual Loss Expectancy (ALE or Expected Value of the Specific Risk) would therefore be $5000, but with an ALE of $5000 it is unlikely that any serious security countermeasures would be put in place. Yet the result of this disaster was devastating. Therefore, this risk assessment approach in this case was meaningless. (World Trade Centre disaster example, personal communication, Jason Taule, October 2004).

Although quantitative data may be available for some disasters (earthquakes, floods, etc.) there is less available on situations such as a 'hacker' breaching a network and 'taking down' a mission-critical system. Therefore, *likelihood* data provides greater utility than *probability*.

4.4 INTERNAL CONTROLS

The countermeasures/safeguards put in place to ensure that the company's internal information is accurate, are referred to as internal controls. Companies have, as part of their risk management, a system of internal controls intended to counteract the inherent risks. Lindberg (2005) points out that internal controls can take the form of operational, financial, or administrative controls. This is in harmony with the research paradigm of this project which highlights Systems Theory principles. One can only apply the system of Internal Controls to the system being addressed (Fig. 1.2). The external environment is not addressed or controlled by the system of internal controls.

4.4.1 Risk Indicators

This approach to risk management includes *risk indicators* associated with specific processes or technologies. The risk indicators point to a need for

controls. Hunton et al. (2004) contend that a company can note the presence or absence of risk indicators for each process, and then choose to control them or not, depending on an analysis as to whether or not the risk is acceptable. The findings of the risk analysis will point to the need for a control objective (internal control).

Both control-based and risk-based approaches are *process-based* and is the method that COSO, CobiT and ISO17799 advocate. It can be explained in a more practical way by considering a process, its *inputs* and the desired *outputs*. Along the way there are various mechanisms (activities and tasks) which are applied to the inputs so that the desired outputs are achieved. However, the process is exposed to various risks, which require managing to an acceptable level by introducing controls.

4.4.2 Overview of Internal Controls

In the late 1980s, public trust in the listed shares of many public companies was damaged due to company failures and investors' lost fortunes. These events led to the establishment of authoritative standard setting bodies for financial services, accounting and auditing professions to asses the nature of the failures. The result was the commissioning of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission (National Commission on Fraudulent Financial Reporting) to conduct a study on company failures and to issue guidance on how to prevent recurrences.

The outcome of COSO's review of internal control systems was the recognition and communication for the need to shift the focus on managing companies from strictly a financial control focus to a focus on managing *"business risks"*. This represented a major paradigm shift in and for corporate boards, management and auditors responsible for auditing and regulatory oversight. COSO believed that by focusing on the broader spectrum of business risks versus solely on traditional financial risks, significant company failures might be minimised in the future.

The COSO report provided a common language regarding controls and created an Integrated Control Framework for managing business risk.

The COSO (1992) Internal Control Framework, which is widely accepted and used extensively, defines internal controls as a process influenced by a company's directors, management and other personnel. It indicates that internal controls are designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Included in the COSO (1992) Internal Control Framework are five interrelated components, integrated within the management process. These components vary in procedure and structure from company to company as they are adapted and customised to meet each company's needs and objectives. It should be noted that each one of these five components relates to the three COSO-ICF categories above.

These five components are:

- **Control environment:** This is the *"tone at the top"* and is management's attitude towards internal controls. This influences whether the company, i.e. its employees, are control conscious or not.
- **Risk assessment:** This is an important part of internal control. Every company faces a variety of internal and external sources of risks. The COSO-ERM Framework (2004) provides companies with guidance in developing plans to identify, measure, evaluate, and respond to risks.
- **Control activities:** These are policies and procedures specific to internal controls. They ensure management's directives are carried out and risks are addressed to enable the company to achieve its objectives. They occur throughout the company at all levels and in all functions.

- **Information** (processing) **and communication:** Relevant information is needed by employees within the company to ensure that strategies and objectives are met as they carry out their responsibilities. This may be internal information within the company or external sources of information from suppliers, customers, shareholders, etc. In addition, there is a need for effective communication in the broader sense, such as flowing up, down and across within the company.
- **Monitoring:** Continuous monitoring of the internal control system is necessary. This assesses the quality and effectiveness of the system's performance over time.

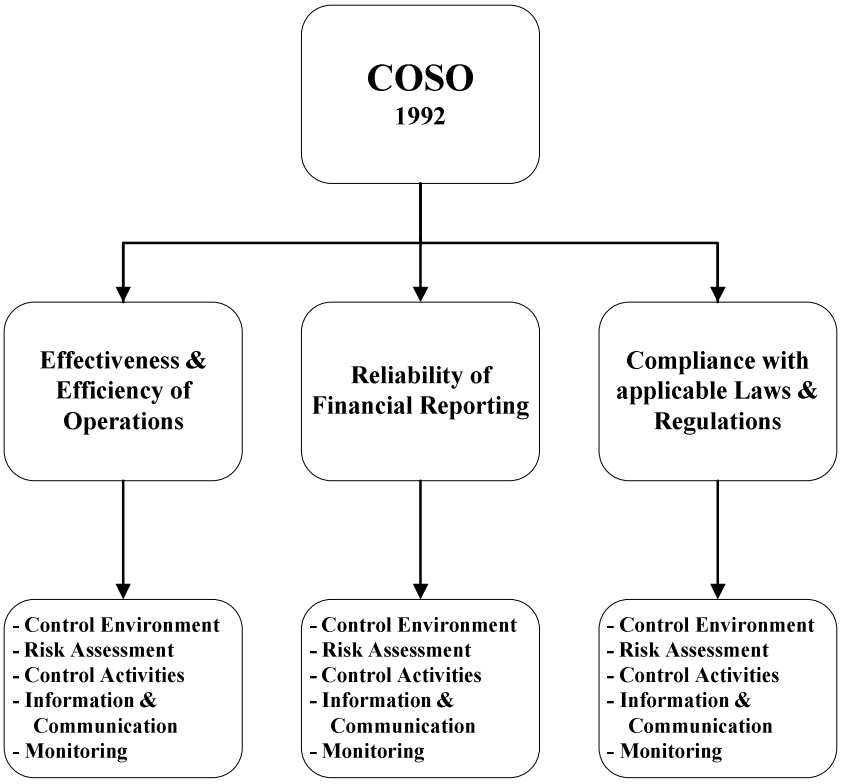

Figure 4.3: An Illustration of COSO's Internal Control Framework

Strong internal controls increase the probability that transactions are recorded correctly, therefore fraud (accuracy) should not occur and the financial

information should be reliable (Flowerday & Von Solms, 2005b). Establishing and maintaining a system of internal controls is the responsibility of management (Hunton, et al., 2004; Braiotta, 2002; Horton et al., 2000; COSO-ICF, 1992). In addition, internal auditors should make recommendations to management for improvements to the controls or procedures, but they are not responsible for the system of internal controls.

4.4.3 IT Controls

Information technology provides opportunities for growth and a competitive advantage for companies. However, it also provides the means and tools for threats to exploit vulnerabilities, be this from outside attackers or from trusted insiders. Fortunately, *IT* can also provide protection from threats. IT controls do not exist in isolation, but form part of the overall system of internal controls (GTAG1, 2005), which in turn is an integral part of enterprise risk management (COSO-ERM, 2004). These IT controls promote reliability and efficiency and allow the company to adapt to changing risk environments (Flowerday & Von Solms, 2005a).

Figure 4.4 illustrates the hierarchy of IT controls. It represents the logical *'top-down'* approach when considering the implementation of controls. It is stressed that the elements shown in the hierarchy are not mutually exclusive, but are all connected and can intermingle (GTAG1, 2005).

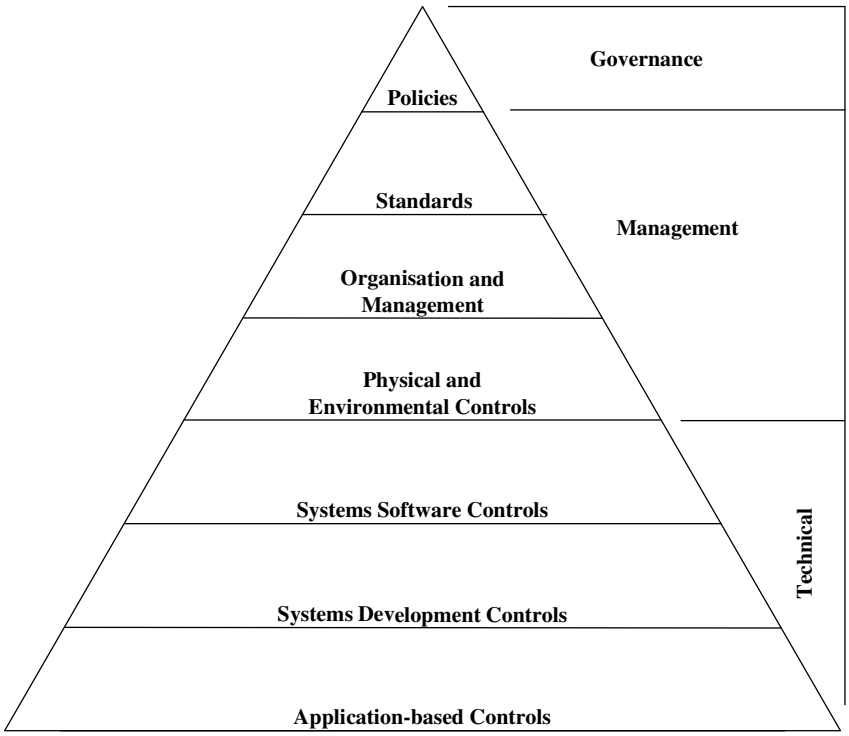

Figure 4.4: IT Controls (GTAG1, 2005)

Stephen Katz (Spafford, 2004), former CISO of Citibank, explained that IT controls do not slow the process down, but are like brakes on a car. The driver is actually able to travel faster with brakes than without because the driver is able to keep the car under control. In addition, the car can be stopped much more rapidly and safely if required. Therefore, the purpose of IT risk management is the identification of a system of internal controls that become the foundation of information *accuracy* and *reliability*.

IT controls have two significant elements (GTAG1, 2005):

- The automation of business
- The control of IT

Hence, IT controls (as shown in Fig. 4.4) support governance and business management as well as provide general and technical controls over policies, processes, systems and people that comprise IT infrastructures (GTAG1, 2005). These include the processes that provide assurances for information and assist in mitigating the associated risks.

The COSO-ERM Framework (2004) classifies IT controls as either *General* or *Application* controls. Flowerday and Von Solms (2005a) help clarify what general and application controls are by elaborating on COSO's explanations and provide the following examples.

- **General controls:** These are also known as general computer controls, information technology controls and infrastructure controls. They include controls over security management, software acquisition, development and maintenance. They support the functioning of programmed application controls and are the policies and procedures that ensure the continued operation of computer information systems, such as backup, recovery, and business continuity.
- **Application controls:** These pertain to the individual business processes, application systems or programmed procedures in application software. Also covered are the related manual procedures designed to ensure the completeness and accuracy of information processing. Examples include: data edits, balancing of process totals, transaction logging, error reporting and manual procedures to follow up on items listed in exception reports.

The function of a control is relevant to the assessment of its design and effectiveness (GTAG1, 2005). Therefore, controls are often categorised into three groups: *preventative*, *detective* and *corrective* controls. CobiT's (2000) Detailed Control Objective DS5.19, titled *Malicious Software Prevention, Detection and Correction,* is a good example illustrating how these controls work together.

In this example, the CobiT control objective deals with malicious software, such as viruses, worms and trojan horses. Business and IT management should have an adequate system of controls established across the company to protect the information systems from malicious software. The control procedures the company implements should include preventative, detective and corrective controls specifically for malicious software and should incorporate incident response and reporting. The following are examples of these three control categories:

- **Preventative controls** prevent unwanted things from happening. For example, CobiT's Audit Guidelines stress, *"all software acquired by the organization is checked for viruses prior to installation and use"*.
- **Detective controls** monitor activity to determine if the preventative controls have failed. For example, CobiT's Audit Guidelines state, *"users have received instructions on the detection and reporting of viruses, such as sluggish performance or mysterious growth of files"*.
- **Corrective controls** return the condition back to the expected state. In other words, if a virus did corrupt a system, the control would reload the applications and the backup or good image, to restore the system to the expected state.

Bletner (n.d.) from the U.S. Navy points out that in military terms they clarify whether something is a *'hazard'* or a *'cause'* before they implement controls (safeguards and countermeasures). The reason for this is that there may be several causes associated with one hazard. Applying this principle to information security when deciding how many and what controls to implement, is important. A hazard in the U.S. Navy can be likened to a *threat* and a cause to a *vulnerability* when compared to information security.

A vulnerability is more specific than a threat (as shown in Fig. 4.2). Bletner (n.d.) uses a question to help him classify a hazard or a cause. Applying this method of clarifying if something is a threat or a vulnerability is to ask Bletner's

question, *"Is this hazard specific enough to help identify a single corrective control?"* If the answer is no, it is a threat; if the answer is yes, it is a vulnerability. It is important to properly identify threats and vulnerabilities because there may be several vulnerabilities associated with one threat. If the more specific vulnerabilities are not identified, necessary controls may be omitted resulting in threats not being mitigated to an acceptable level and therefore the system of internal controls is inadequate.

Figure 4.5 illustrates how the various controls work together and interact as *a system of internal controls*. This figure helps to classify and understand the control's purpose and where it fits into the overall control system.

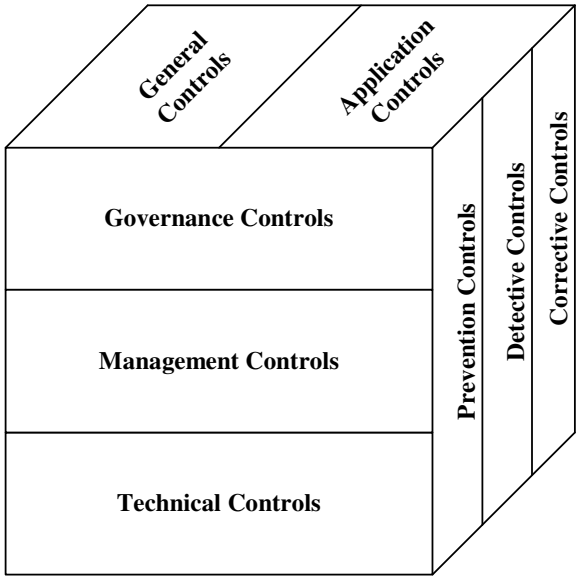

Figure 4.5: Control Classifications (GTAG1, 2005)

It can therefore be concluded that a system of internal controls assists the directors in fulfilling their responsibility in protecting the company's assets (especially information assets) from internal or external threats and direct or indirect threats. If one considers the operational risk definition, a thorough system of internal controls can help meet the specified requirements. Additionally, if one reflects on the Basel II Accord and the Sarbanes-Oxley Act

(these two are used merely as examples to illustrate the *trend* of the 'codes') a system of internal controls, provided there is some form of real-time monitoring and reporting system, can help with compliance with these codes and others. A system of internal controls has become core to the company's risk management practices and assists the directors in their decision making process as they *guide and steer* the company towards its goals and objectives.

4.4.4 Control Standards, Frameworks, Models and Guidelines

There have been various control standards, frameworks, models and guidelines developed and proposed over the years. This research project will refer to these collectively as *standards*. These standards help a company comply with the *codes* discussed in Chapter Two. However, once a company has completed its risk analysis process it needs to design its own customised control framework (providing guidance, policies and processes) to address its risks. Once the company's control framework has been designed and agreed upon, the company should build an internal control system (the interactive pieces that enable the operation of the framework).

A few standards which assist a company in setting up their own internal control framework are: COSO, CobiT, ISO/IEC 17799, ITIL. In many instances, a company will use a combination of, or parts from, a few of these standards in designing their own control framework (Oud, 2005; Spafford, 2004). Figure 4.6 by Flowerday and Von Solms (2005a) illustrates how these standards can complement each other as they tend to focus on different areas. Information security practitioners and auditors use these standards extensively when establishing and evaluating internal controls.

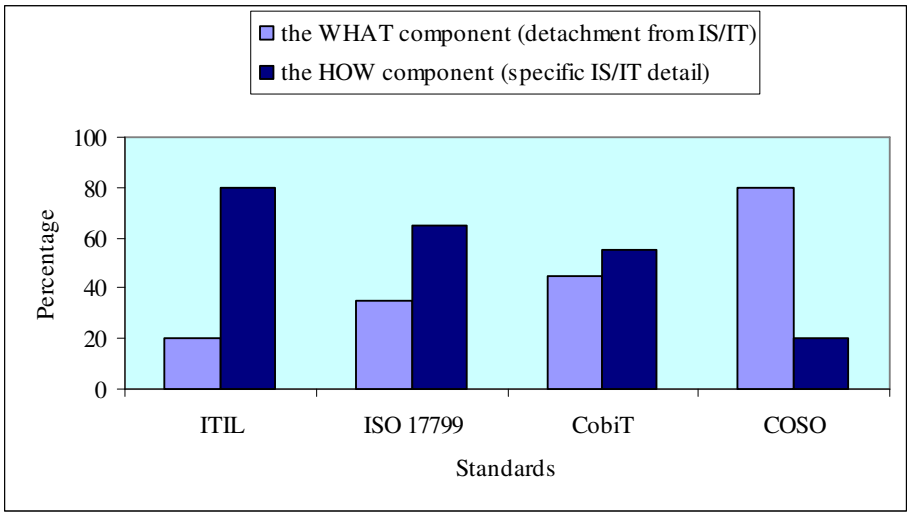

Figure 4.6: A General Guide that Illustrates the Standard's Tendency Towards IS/IT or Business (Flowerday & Von Solms, 2005a)

4.4.5 Real-time Monitoring System

Once the system of internal controls is in place and working, its effectiveness needs to be monitored to ensure that the controls are satisfactory and functioning correctly. Ninety percent of the participants of a survey carried out by the Computer Crime Research Centre (CCRC, n.d.), covering a twelve month period for 2005, reported unauthorised intrusions as a result of exploitation of known vulnerabilities of which there are known countermeasures available (CCRC, online 4 February 2006). Eighty percent of these survey participants reported financial losses due to the security breaches. PwC, in their survey, have the figure slightly lower at eighty-four percent of respondents who reported security breaches (Ware, 2002).

In the first six weeks of 2005, sixty-three percent of companies reported that they were 'attacked' and had network security problems. Virus and worm attacks lead the list of intrusions followed by Trojans (Amplitude Research, 2005). A security breach, as classified by the CCRC, is the *"successful and attempted security breaches, theft, financial fraud, and virus detection"*.

As stressed by Flowerday and Von Solms (2005a), this monitoring *overlay* assists management by assuring themselves that their 'checks and balances' are in place within their business processes. They also note that, to be truly effective, the system should be in real-time. This system also reassures management that their business transactions are recorded soundly and the risks are contained. One should not assume that because the company has created an *adequate* set of internal controls that the controls are always working properly. It is very important that internal controls are continuously checked for efficiency and operational effectiveness.

As noted previously, compliance to regulations such as Sarbanes-Oxley and Basel II, augment the need for systems of internal control and disclosure controls on financial and operational processes. The company's system of controls should highlight transparency not just for boards and management, but investors and the various stakeholders alike. The various stakeholders ultimately need assistance in determining if their company's risks are being addressed.

Therefore, director-level 'dashboards' could be established that would have real-time information fed to them from the bottom-up, to provide readings. The company could be better managed from the very top; these senior managers would receive current reliable information from 'grassroots' on the information security and related risks. Managers would be kept continuously informed and the speed at which information would flow throughout the company would be greatly increased. Performance could be monitored, measured and reported on and therefore, performance could be improved.

4.5 EVOLUTION OF OPERATIONAL RISK MANAGMENT

The evolution towards a more comprehensive risk management model for managing operational risk and thereby reducing uncertainty and vulnerability is taking shape. To be effective, 'Enterprise Risk Management' (as termed by

COSO-ERM) must be holistic and forward looking, not just dealing with historical data. It should address all the risks the company faces.

Figure 4.7 illustrates how *uncertainties* in the operational and specifically IT risk arena are addressed through risk management. The risk management process reduces *vulnerabilities* and helps to predict a favourable future outcome. Based on *predictability,* the financial statements of the company can therefore be assumed *accurate* and *reliable* until assurances are provided by auditors. One can conclude that the accounting and financial information systems can be trusted and the various stakeholders can build and establish *trust* between them in this domain. Therefore, *confidence* can be placed in the financial statements when making decisions.

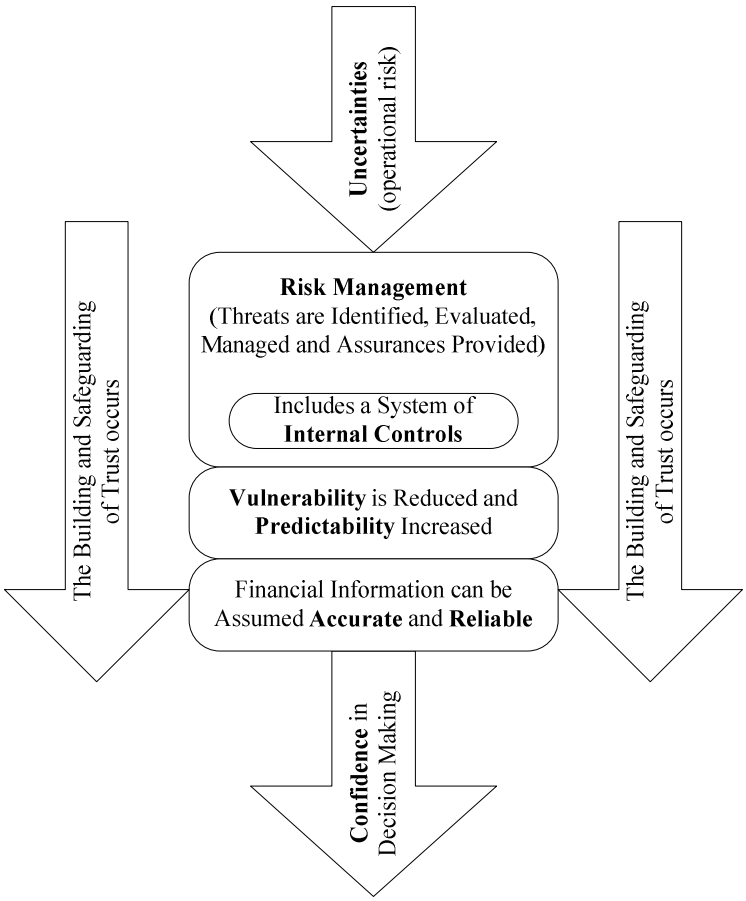

Figure 4.7: Uncertainty – Risk Management - Confidence

Having noted the importance of these codes, they are not without their critics. The Sarbanes-Oxley Act has received a great deal of criticism due to its increased financial burden and costs that companies must bear in achieving compliance. The companies are retaliating and lobbyists are active in Washington DC claiming that this Act is *"debilitating to businesses*" (Solomon, 2005; Rich, 2006). In addition, there are companies which have unlisted or are looking to unlist from US stock exchanges rather than comply with the Act. The Act's 'burden' seems particularly heavy for smaller companies and appears to restrict their access to financial capital (Solomon, 2005; Sorkin, 2006; Fleischer, 2006). A version of the Act called SOX-Lite is being considered for smaller companies and particularly the European countries are lobbying for this, focussing their efforts on section 404 (Feldman, 2005; Garai, Mason, Levinson & Thompson, 2005).

The Basel II Accord is also not without its critics, especially the section on operational risk. As pointed out by Leeladhar, managing risk is increasingly becoming the single most important issue for the regulators and financial institutions. Yet the techniques and suggestions in this Accord pose considerable implementation challenges and can be described *"as a long journey rather than a destination"* (Leeladhar, 2005). This code has many critics, however, in that most are critical of the complexities and difficulties found in the implementation and the time scales attached to compliance (Westlake, 2003) rather than the principles of the code.

The trends are clear that operational risk and IT risk as a subsection need to be addressed. They will not go away. Influential *codes* such as the Sarbanes-Oxley Act and Basel II Accord act as powerful drivers on the compliance side and *standards* such as CobiT and COSO are prominent implementation guides. Regardless of the implementation complexities and whether implementation timescales are delayed or not, the inevitability of managing operational risk, aided by a system of internal controls, will continue to evolve and grow. This

will assist in reducing future business risk uncertainties and ensuring accurate and reliable financial information.

4.6 CONCLUSION

Operational risk and especially the focus of this research project on IT risk has become increasingly important in recent years. Information security management, which includes a system of internal controls, has become paramount to operational risk management. IT therefore can become a tool to assist in visibility and transparency as it supports business processes and the various systems belonging to the company.

Companies need systems that increase visibility into their business processes. The directors then become more aware of the information risks they are exposed to due to the increased visibility and transparency. Consequently, the company has greater insight, using 'dashboards' into the make-up of these risks at a deeper and more detailed level. As a result, directors and investors gain confidence in the financial statements that senior management are required to certify. The transparency enables genuine accountability and as a corollary, leads to better management decisions, once again adding value.

Furthermore, uncertainty is reduced to an acceptable level as predictability increases. The real-time monitoring of the company's system of internal controls assists in building trust that the system is effective and efficient. Thus, this system of internal controls assists in ensuring that information found within the financial processes, is accurate and reliable.

This chapter is important to any company that has the goal of practising good governance. To practise good governance, *all* risks need to be managed. The various information systems need to be trusted and sound risk management practices, including a system of internal controls, helps with achieving this.

This leads to the next chapter which focuses on the Audit Committee and how it helps to provide assurances that the financial statements are a *fair representation* of the company. This important committee is there to assist both the *Agents* and the *Principals*. The Agents receive assurances from the audit committee that management's risk management practices, including a system of internal controls, are effective and efficient. The Principals (investors) receive assurances that the board of directors (agents) are governing the company in an appropriate way and the financial statements reflect the 'true' condition of the company.

Chapter 5

AUDIT COMMITTEE

"It isn't that they can't see the solution. It is that they can't see the problem."
- Gilbert Keith Chesterton, (author, 1874 – 1936)

5.1 INTRODUCTION

This chapter is necessary to this thesis because it highlights the important governance principles of *accountability* and *responsibility*. These two important principles of corporate governance are addressed as one considers the role of the audit committee. *Transparency* and *fairness* are also principles of importance to the audit committee, and auditors help address these latter principles. This chapter helps a company establish good governance in the area of financial reporting.

In Chapter Two, the importance of accurate and reliable financial statements was discussed as an important element of governance. As stated in Chapter Three, for trust to grow, uncertainty needs to be reduced and predictability needs to increase. This led naturally to the management of risk as this helps to mitigate unexpected and unfavourable future events that may cause uncertainty. Reduced risk allows increased trust.

Current risk management practices were addressed in Chapter Four where a system of controls was emphasised. Additionally, Chapter Four demonstrated how internal controls assist a company in achieving its business objectives as it 'protects' the company from threats which may cause harm and uncertainty.

Furthermore, Chapter Four argued that the company's information systems need to be trusted and the system of internal controls assists with this.

This chapter introduces the concept that the auditors validate the company's financial statements and systems by 'evaluating and assessing' the *accuracy* of the information for intentional or unintentional errors. In addition, auditors validate the financial information's *reliability*, which includes the integrity of the information and the data that makes up the information. The latter is accomplished in part by evaluating the company's system of internal controls.

However, companies rely increasingly on electronic information. Technologies such as EDI (electronic data interchange) or EFT (electronic file transfer) convert traditional accounting systems into paperless systems. With the traditional audit trail disappearing, it is becoming commonplace for auditors to use technology to assist them in their duties and responsibilities.

The auditing principles require that the electronic financial information needs to be audited and assurances given. The auditors then become an independent source providing information as to the *'condition'* of the system or information audited. The overall responsibility for this process rests with the board of directors; however, there is a subcommittee of the board that assists with this responsibility.

The audit committee, a subcommittee of the board discussed in this chapter, has become a key committee in recent years in a move to improve financial reporting and governance. The role and responsibilities of the audit committee are discussed in more detail as the decision makers and users of information require assurances for the information on which their decisions are based.

5.2 AUDITING

The auditing process is conducted by 'independent' auditors who express opinions and provide *"reasonable assurances"* after the audit has been concluded. This process allows the decision makers who base their decisions on this information, confidence when making their decisions.

5.2.1 What is Auditing?

Auditing is a profession where auditors examine information and verify records, systems, and reports. During their examination, they identify areas where the accuracy and reliability of the information is *'judged'* and thereby provide an independent opinion as to the condition of the information. An appropriate formal definition is: *"Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria"* (Arens, Elder & Beasley, 2003, p.11).

To conduct the audit there must be information in a verifiable form and some criteria (standard) by which the auditor can evaluate the information. It is important that at this stage one should not confuse accounting and auditing.

Accounting is the recording, classifying and summarising of economic events in a logical manner providing financial information for decision-making (Arens et al., 2003). Conversely, auditing the accounting data and information is concerned with determining whether recorded information properly reflects the events that occurred during a specific period.

As pointed out, the nature of the audit process has changed as the majority of source documents and the evidence trail has changed from a paper form into an electronic format. To audit electronic systems, auditors have taken advantage of the advances in technology and incorporated audit software into the audit process to assist them in gathering and analysing evidence. Additionally, auditors use

software to assist them in assessing the risks introduced by IT, databases, the Internet, and other technologies.

These developed technologies are often referred to as audit tools and techniques and assist the auditors in fulfilling their responsibilities. They allow the auditors to examine all of a company's records, not just a sample, if they so wish. CAATTS (computer assisted audit tools and techniques) enable the auditor to perform data extraction and analysis more efficiently and thereby increase the effectiveness of the audit and the productivity of the auditor (Flowerday & Von Solms, 2005a).

CAATTS can be separated into two groups: one that focuses on audit *tools* and the other on audit *techniques*. The *tools* (generalised audit software or GAS, expert systems, statistical analysis, etc.) comprise software that increases the auditor's productivity and ability to manage the audit. The *techniques* (data query models, embedding audit modules, test decks, etc.) validate applications, verify data integrity and test the effectiveness of the internal control system (Cangemi & Singleton, 2003; Hunton et al., 2004).

The audit profession consists of both internal and external auditors and both use CAATTS. To clarify the distinction between these two sets of auditors, their respective focus and responsibilities will be discussed in brief. However, this thesis refers to auditors in general and does not focus on either group specifically.

External auditors are independent of the company. They must be independent in both fact and in appearance. These auditors provide auditing services on a fee basis. External auditors do not alleviate the need for the internal audit function or vice-versa. The services provided by both internal and external auditors are complementary (Cangemi & Singleton, 2003; Hunton et al., 2004).

The responsibility of internal auditors is to give management an independent, objective and fair view of the company's activities. They are employees of the company. In addition, these auditors meet on a regular basis with the audit committee to address management, control, and assurance issues. An important part of their responsibilities is that of assessing the internal control system (Cangemi & Singleton, 2003; Horton et al., 2000; Hunton et al., 2004).

5.2.2 Auditing Information Systems

In recent years, auditors have shifted their approach to using their expertise gained over the decades to controlling risk. Auditors have moved from a control-based audit model to a risk-based model (Arens et al., 2003; Bierstaker, Burnaby & Thibodeau, 2001; Houck, 2003; Hunton et al., 2004). Rather than just controlling, auditors evaluate risks related to the company's strategy and objectives by selecting cost-effective controls that best mitigate the company's risks.

In addition, auditors have moved from *'auditing around the computer'* and now assess and test the IT controls, as well as the computer input and output data to ensure its integrity. No longer is the computer seen as a 'black box' and assumptions made that inputs and outputs are naturally correlated. However, it does appear that auditors lack confidence in their technical abilities in doing this sufficiently (Braun & Davis, 2003; Houck, 2003).

To illustrate risk-based auditing within an automated business process using information systems such as ERP systems, the following example is used. It is important to note that when conducting the audit an understanding of the objectives of each business process is required. These objectives need to be incorporated into the business process while adequately considering the risks and internal controls. DeMaio (2001) adds that management should set and agree upon the control objectives for the various parties and emphasises that these controls should be rigorously tested and assurances given.

For example (Bierstaker et al., 2001), a sales process of a manufacturing client would include the purchase of raw materials, the manufacturing of inventory, the selling of finished goods and the collection of accounts receivable. Rather than auditing by department, process auditing can cut across multiple departments. This process audit should also refer to the business process performance measures. These performance measures help an auditor gain an understanding of the key business processes that must be in place for a client to accomplish their goals and then determine whether such processes are operating effectively and the risks managed.

As ascertained earlier, the paper trails and control checkpoints once standard for an audit are now only available in electronic formats. If traditional methods of testing controls continue to be used, significant risks may go unnoticed (Bierstaker et al., 2001). The audit software packages assist the auditors by improving their efficiency by automating tasks. Examples are that the software continuously monitors for high risk transactions, internal controls, inventory trends, unusual items (amounts/values over a certain limit) and other key performance indicators (Bierstaker et al., 2001)

The technology impact on auditing is having an effect on the planning and carrying out of the audit. Generic audit templates for specific processes are becoming available and refined as the auditor inputs data into a computer questionnaire, which helps to identify internal control strengths and weaknesses. The computer then helps to analyse the data and determines if the present system of controls is adequate or if there are controls missing by benchmarking against industry standards. This is part of the process of determining if the risks the business process is exposed to are adequately addressed.

This approach assists the auditors in their task of assessing evidence which is transmitted in electronic format. The auditor audits 'through the computer' and information systems to gain assurance that the evidence has not been altered. According to AICPA (1997, p.2) *"the competence of electronic evidence usually*

depends on the effectiveness of internal control over its validity and completeness". This business process analysis approach provides the auditor with an understanding of the internal control environment and therefore the auditor can determine how much evidence must be collected and evaluated before a report can be issued.

5.3 ASSURANCES

"Assurances services are independent professional services that improve the quality of information for decision makers" (Arens et al., 2003, p.4). Independent auditors can add value by providing assurances about the quality of security and the control environment as the various company stakeholders often have incomplete information as to their information's condition. These audits then provide an insurance effect as the auditor assumes some of the risk (Morris, 2002).

In fact, this was the case with Enron and Arthur Andersen (Freedom of Information Centre, 2002). When Enron collapsed, it affected their auditors because Arthur Andersen had not provided a 'fair representation' of their client once audited. Therefore, they assisted the *agents* in misleading the *principals;* the repercussions of this behaviour was detrimental to Arthur Andersen, and they too collapsed.

Almost as an automatic response to the Enron/Arthur Andersen, among other debacles, the Sarbanes-Oxley Act was passed which includes a section (Section 302, p.65) clearly placing the responsibility for financial reporting at the very top of the company. This section does not just hold the CEO and CFO responsible for establishing and maintaining internal controls, as noted in Chapter Four, but also *materiality*. This requires that the signing officers (CEO and CFO) state that, based on their knowledge, the financial statements *"fairly present in all material respects the financial condition and results of operations"*.

The OECD (2004, p.25) states that the board's responsibilities include *"ensuring the integrity of the corporation's accounting and financial reporting systems"*. The OECD continues and specifies that these responsibilities comprise an:

- independent audit,
- appropriate systems of control,
- systems for risk management,
- financial and operational control,
- compliance with laws and relevant standards.

The King II Report (2002) is in accordance with both the OECD and Sarbanes-Oxley in placing the ultimate responsibility for the company's financial reporting with the board of directors. This illustrates the importance of the audit committee, which assists the CEO and CFO in fulfilling their fiduciary duties. The board of directors need assurances that they have fulfilled their responsibilities and due diligence and care is carried out.

To continue with assurance services, one category is *Attestation Services*. An attestation service is a type of assurance service in which the auditors issue a report about the reliability of an assertion that is the responsibility of another party (Arens et al., 2003). Traditionally, the attestation services were concerned with auditing or reviewing *historical* financial statements. However, today there are other attestation services as some of these are natural extensions of the audit of historical financial statements. Today, users want '*data on demand'* and the users seek independent assurances about various types of information. These include information about internal controls relating to financial reporting.

This approach of auditing is forward looking compared to historical auditing. It is forward looking because an effective system of internal controls reduces the likelihood of *future* misstatements in the financial statements. Boritz (2005) is in agreement with this and contends that today assurance efforts of auditors should go beyond financial information and address operational and managerial information.

This *preventative* approach, to use a security term, is in harmony with all forms of assurance services, including audits and attestation services. Assurance services should focus on improving the quality of information used by decision makers (Arens et al., 2003). Thus, a party will be considered trustworthy if there is sufficient credible evidence leading one to believe that set given requirements are met (Sinclair, 2005). This is in line with the theory discussed in Chapter Three where increased predictability reduces uncertainty about future events and therefore assists in building trust between the various parties.

Independent auditor's assurances are likely to increase confidence between the various parties as they base their decisions upon the information made available to them. To stress: the audit process monitors performance against agreed set targets. The auditors then provide the truth or a true picture. Thus, uncertainty can be reduced and trust between the various parties can 'grow'. However, an important question to ask is how are auditors independent if they are appointed, report to, and paid by the directors? This question leads to the next section, the Audit Committee.

5.4 THE AUDIT COMMITTEE

The board of directors have various committees that advise it and report on the company. Through these committees, the directors remain informed as to the company's conduct and performance. These committees *"allow the board to properly discharge its duties and responsibilities and effectively fulfil its decision taking process"* (King II Report, 2002, p.72). One such committee is the Audit Committee.

5.4.1 Audit Committee Responsibilities

This committee is defined as a subsection of the board, designated with oversight responsibility to include: (1) internal controls, (2) financial reporting and (3)

auditing. To reiterate, the audit committee is representative of the full board of directors (DeZoort, 1997).

In Chapter Two, Agency Theory was discussed because it highlighted the conflict of interest between principals and agents (Berle & Means, 1967). The inability of the principal to directly view the agent's activities has helped provide justification for the existence of the audit committee. Jensen and Meckling (1976) identify contractual relationships between principals and agents as a means of curbing agency costs; however, these contracts must be subsequently monitored. This subcommittee of the board assists with this monitoring.

A committee based in the USA produced an influential report in 1999 (since updated in 2004). This committee is known as the Blue Ribbon Commission on Audit Committees (NACD, 1999; NACD, 2004). It made ten recommendations regarding the audit committee's construction, improved audit effectiveness, definition of accountability of the audit committee, management and outside auditors. The purpose was that of improving the oversight process and minimising the potential for abuse of discretion. It therefore becomes possible to increase financial reporting accuracy and reliability. Thus, the ultimate goal of the committee according to Millstein (1999, p.1060) is to ensure that *"independence, awareness, diligence, and care were the primary principles governing the unavoidable exercise of discretion"*.

Among the ten recommendations made by the Blue Ribbon Committee for Audit Committees are that they must have a *"self-regulatory framework emphasizing disclosure, transparency and accountability"* (Zacharias, 2000). The Blue Ribbon Committee specifically recommended strengthening the independence, effectiveness, and accountability of the audit committee. The various recommendations made by the many 'codes' (Cadbury, 2002; King II Report, 2002; Sarbanes-Oxley, 2002) and committees have substantially increased the audit committee's profile and responsibilities.

For example, the Sarbanes-Oxley Act (2002) influences the audit committee by giving it a higher profile and by emphasising its independence of the board and stresses that the board should not influence the committee's findings. According to the Act, the committee has direct oversight for both the internal and external audit function and must be awarded the appropriate funding to function properly, including authority to hire additional advisors if so required.

The King II Report (2002, p.140) affects the audit committee by stressing that the majority of its members should be independent non-executive directors. These members should be financially literate and should not be on the committee as a result of *"cronyism or tokenism"*. In addition the audit committee members should be disclosed in the company's annual report and the chairperson of the audit committee should attend the company's Annual General Meeting to answer questions about the committee's work.

To continue with the responsibilities of this important subcommittee, DeZoort (1997) conducted empirical research based in part on Wolnizer's 1995 study of audit committees. His objective was to clarify the oversight responsibilities of the audit committee. According to DeZoort (1997), the oversight responsibilities pertained to *financial reporting*, *auditing* and *corporate governance*. The study concluded by prioritising the audit committee's oversight responsibilities in the following order. These were (1) *internal control evaluation* followed by (2) *financial statement review* and then only (3) *auditor evaluation* (both internal and external).

In fact, DeZoort's findings consistently ranked internal control evaluation as the most important oversight responsibility and was conducted using a multi-method research approach. DeZoort's findings are in line with the Blue Ribbon Committee that reported that the three major areas of the audit committee's responsibilities are: *financial reporting*, *risk management*, and the *audit function*. As covered in Chapter Four, risk management primarily relates to a company

system of controls and therefore falls under the audit committee's oversight remit.

Considering audit committee oversight responsibilities, the King II Report (2002, p.140-141) emphasised the review of the:

- system of internal controls,
- internal audit department,
- scope of the company's operational risk areas to be covered in both the internal and external audits,
- *reliability* and *accuracy* of the company's financial information,
- any auditing or accounting concerns identified as a result of audits,
- compliance with legal and regulatory provisions including rules established by the board.

According to Spira (2003) since the Cadbury Committee's 1992 report, audit committees have become a standard feature of corporate governance in the UK for listed companies. Ultimately this subcommittee of the board, representing the full board, is charged with the oversight of the company in almost a 'watchdog or policing' function.

5.4.2 Audit Committee and Risk

As a means of fulfilling its oversight function, the audit committee must therefore ensure that management has fully assessed all of its risk and maintains an effective risk management framework (COSO-ERM, 2004). To concur, the committee would be negligent in providing due care if it failed to ensure that management discharged their risk management responsibilities without going through a thorough risk analysis of all risks (voluntary and involuntary) facing the company (Horton et al., 2000)

At the director's level, the audit committee generally takes the lead in overseeing many key business risks. As noted, the expectations placed on audit committees have risen dramatically in recent years as they assist the board in fulfilling their risk management responsibilities.

An audit committee survey conducted by Ernst & Young in South Africa (IIA Adviser, 2006, p.17) found that *all* of the companies surveyed now have audit committees (large companies were surveyed). Additionally, they found that the independence of internal audit departments has increased as now almost 70% of the heads of these departments report to the audit committee. They also discovered that the audit committees are calling for *"… education in terms of understanding Enterprise Risks to be improved"*.

Even though the King II Report (2002, p.72) stresses that a company's board of directors should have, at the minimum, an audit and a remuneration subcommittee, the Ernst & Young survey found that 75% of companies either had or were setting-up Risk Committees. The literature survey conducted during this research project found that there is growing evidence of the importance of a Risk Committee operating as a subcommittee of the board of directors.

The King II Report (2002, p.70) states that a company may consider having a risk committee, however, it does not go into detail. The Sarbanes-Oxley Act of 2002 does not even refer to a risk committee. This may be because the focus of the Act is on financial reporting and audit committees tend to take the lead on financial, audit and control issues. For this reason, the audit subcommittee of the board is of importance to this research project which focuses on these important issues.

Moreover, it is noted that some companies and organisations have implemented an *"Audit and Risk Committee"* as a single committee (ACPET, 2006; Iluka Resources Limited, 2005; QltInc, 2006). Then there are others that have implemented them as separate committees and therefore have an Audit Committee and a Risk Committee. In some of these cases, the Risk Committee reports to the Audit Committee (Deutsche Bank, 2004; Mellon, 2006; Toronto-Dominion, 2005). However, not all companies have done this as some operate

with only the Audit Committee. For the purpose of this thesis, reference to the audit committee shall mean audit and risk committees.

5.4.3 Audit Committee's Responsibilities within the IT Arena

Since part of a company's risk assessment involves IT along with its associated risks, these risks must be assessed by management subject to internal and external audit review. As already stressed, ultimately the board oversight, namely the audit committee, is to ensure that the management of IT Risk is carried out effectively.

Clearly, information technology has permeated all aspects of the company creating a substantial dependency and interdependency. According to SysTrust, IT systems must therefore remain secured, available as required, and capable of producing consistent information with integrity (AICPA & CICA, 1999). Moreover, the audit committee can act as an arbiter between management and the auditor (King II Report, 2002). The committee must gain assurance that the auditor possesses, or has access to sufficient, competent audit resources to evaluate information security and the associated risks (Horton et al., 2000).

As already discussed, according to the Blue Ribbon Committee and DeZoort, one of the audit committee's top priorities is the assessment of the company's internal controls (including IT Controls). Hence, this is fundamental in fulfilling the committee's fiduciary duties and responsibilities. Again Horton et al. (2000) stress that providing sufficient information security oversight under its due care duties, the board (namely the audit committee) must ask critical questions of management to ensure that internal controls are adequate.

Figure 5.1 is a high level flow chart that illustrates the management and auditing process (Flowerday & Von Solms, 2005a). It shows that management is responsible for the system of internal controls and that the auditors will audit both the system of internal controls and the financial data and information. Bear

in mind that to have information integrity both the system and the data need to have integrity; however, this will be discussed in more detail in Chapter Six.

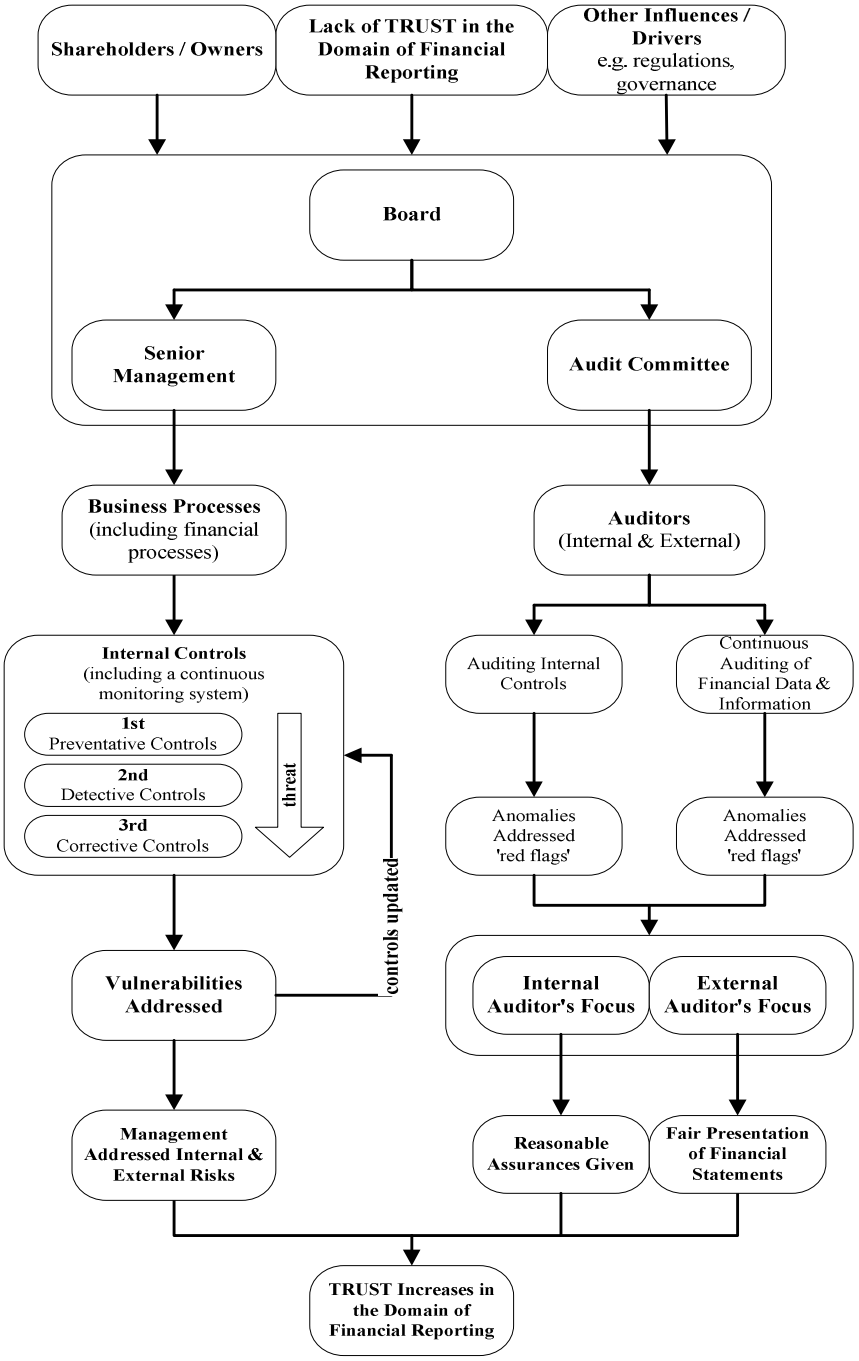

Figure 5.1: High-level Flowchart Illustrating the Management and Audit Processes (Flowerday & Von Solms, 2005a).

To reiterate, the audit committee is to consider the effectiveness of the company's internal control system, including that of its information systems. The COSO-ERM report (2004, p.64-65) has classified information system controls into two broad groupings: General and Application Controls. This report states that these controls, *"combined with manual process controls where necessary, work together to ensure completeness, accuracy, and validity of information"*.

The audit committee is also to understand the scope of the internal and external auditor's review of internal controls over financial reporting. In addition, it is to obtain reports on significant findings and recommendations, together with management's responses. Given that most operational processes, especially those supporting the company's finances, are automated and use information technology, one cannot emphasise the internal controls for information technology enough. Moreover, today it is accepted that IT systems are inextricably linked to the financial reporting processes (IT Control Objectives for Sarbanes-Oxley, 2004).

To assist the auditor in understanding and assessing IT Controls, Figure 5.2 graphically illustrates the structure of IT auditing. As pointed out by GTAG1 (2005), business processes are constantly changing and technologies evolving which enable new threats to emerge as new vulnerabilities are discovered. Therefore, the assessing of IT controls is a continuous process and not an event.

GTAG1 stresses that management provides IT control metrics and reporting. The auditors then audit and attest to the IT controls validity and report on their value. As noted in Chapter Four, IT controls do not exist in isolation, but form part of the overall system of controls. Also IT controls, like other controls, are subject to error and management override. However, GTAG1 (2005) highlights that IT controls support the concept of *"defence in depth"* so a single weakness does not always result in a single point of failure.

The focus of the IT controls should therefore be to provide assurances for information systems and services and help mitigate the risks associated with the company's use of information technology (Champlain, 2003; Houck, 2003).

GTAG1 (2005) points out that the auditor's role begins with a conceptual understanding and culminates in providing the results of risk and control assessments concerning these controls. They continue that these controls range from written corporate policies to their implementation with coded instructions. It is stressed that the assessment should be *holistic* in that it should include physical access protection with the ability to trace actions and transactions to the individuals responsible for them.

To summarise: *"Assurance must be provided by the IT controls within the whole system of internal control and must be continuous and produce a reliable and continuous trail of evidence"* (GTAG1, 2005, p.3). As discussed, IT auditors use various tools and techniques to enable them to perform various tests when assessing the adequacy of IT controls. Figure 5.2 illustrates the areas the auditor needs to consider and where this section fits together in assessing IT controls.

Assessing IT Controls		
	Understanding IT Controls	**Governance, Management, Technical**
		General / Application
		Preventative, Detective, Corrective
		Information Security
	Importance of IT Controls	**Reliability and Effectiveness**
		Competitive Advantage
		Legislation and Regulation
	Roles and Responsibilities	**Governance**
		Management
		Audit
	Based on Risk	**Risk Analysis**
		Risk Response
		Baseline Controls
	Monitoring and Techniques	**Control Framework**
		Frequency
	Assessment	**Methodologies**
		Audit Committee Interface

Figure 5.2: The Structure of IT Auditing (GTAG1, 2005)

To emphasise, the influential COSO-ERM report (2004) refers to the specific controls within the company's applications, such as ERP systems, that help to control the processing as Application Controls. These application controls are a broad group of controls that *"focus directly on completeness, accuracy, authorization, and validity of data capture and processing"*.

If one considers COSO's approach, the controls within a business process need to be assessed. There are various control frameworks (standards as referred to in Section 4.4.4) which can assist the auditors to carry out their responsibilities, one of which is CobiT (2004). This 'standard' provides guidance for the company

with the ability to assess the overall IT risks on a continuous evaluation basis. Furthermore, this standard guides the company in their achievement of business objectives based on this process approach. Thus, *reasonable assurances* can be provided if the company uses, assesses, and implements CobiT together with other standards, as discussed in Chapter Four, and thus establishing a *holistic risk management approach*.

One of the reasons that CobiT is such a useful 'standard' is that it is strategically orientated and allows the company to effectively develop information systems to support the company's strategic processes and business objectives. Once these strategic information systems are in place, a system of internal controls can be designed to support the business processes and systems, at the same time managing the risk exposure.

Subsequently, the assessment of the internal controls can be preformed. This standard can assist in assuring that IT Risk is managed adequately. In addition, CobiT is an effective governance guideline (together with others as discussed in Chapter Four) and assists the company in complying with the various 'codes' such as Sarbanes-Oxley, Basel II and the King II Report.

5.5 CONCLUSION

Auditors must keep pace with the fast moving world of technology, and auditing software should be used during the audit process. Today's risk-based audit model should focus the auditor's attention on internal controls in an effort to prevent threats from exploiting vulnerabilities in the company's automated business processes.

For assurances to be provided as to the condition of the financial information, auditors need to 'evaluate and assess' the electronic information as the paper trail continues to fade. Auditing 'around the computer' is not acceptable and auditors are expected to 'audit through the computer' and information systems.

The audit committee is a crucial committee in providing a monitoring role and establishing good governance. This subcommittee of the board of directors is responsible for *risk management*, *financial reporting*, and the *audit function*. In addition, this important committee allows the *Principals* some degree of 'security' in knowing that the risks the company faces are being managed effectively and that the *Agents* are not conspiring against them.

The quote at the very beginning of this chapter is important because even though auditing has advanced to the stage it has, it still does not produce assurances in real-time. The problem still exists that the decision makers often base their decisions on real-time information where assurances are not available, therefore uncertainty and risk is present. Nevertheless, a proposed solution will be discussed in Chapters Seven and Eight. However, information integrity needs to be established, and this discussion will follow in Chapter Six.

Chapter 6

INFORMATION INTEGRITY

"Integrity without knowledge is weak and useless, and knowledge without integrity is dangerous and dreadful."
- Samuel Johnson, (writer and poet, 1709 - 1784)

6.1 INTRODUCTION

The auditing profession has adopted the concept of *reasonable assurance*. This concept requires that the auditors perform enough work to obtain reasonable assurance that the information found within the financial statements of a company is free from materiality and is a *fair or faithful presentation* of that company's financial position. It is argued by critics who oppose the concept of reasonable assurance in favour of absolutes, that this is a way for auditors to reduce legal liability. Houck (2003, p.16) however contends this is unfair and asserts that: *"Reasonable assurance is a commonsense, cost-effective concept that enhances the integrity of financial reporting"*.

This chapter focuses on information integrity, however, it is acknowledged that 100% information integrity is not currently achievable due to various limitations and therefore the auditing concept of *reasonable assurance* will be adopted. This is in line with the concept that 100% information security is not achievable and the notion that *adequate security* is the goal, using appropriate countermeasures. Absolutes in many cases, including *absolute trust*, in this imperfect world is not achievable, therefore the concept of *"acceptable*

uncertainty" should be the objective (personal communication, Alex Todd, July 2005).

The main contribution of this chapter is to illustrate the importance of and provide a macro view of what constitutes information integrity. However, to understand information integrity it has been necessary to firstly attempt to clarify what is data and information as well as to understand quality even if at a basic level. This then enables the discussion to move forward onto the focus which is information integrity.

Therefore, the chapter starts with investigating what is data, followed by information and knowledge. It then briefly discusses information and communication theory and highlights the link between the two. The concept and attributes of data and information *quality* are presented. This leads naturally into the 'core' attribute which is *information integrity*. The attributes of information integrity are explored and it is noted that to have information integrity, both the *data* and the *system* need to have integrity.

6.2 DATA, INFORMATION AND KNOWLEDGE

It appears at times that the use of the words *data* and *information* are used 'loosely' and some use these words interchangeably. Additionally, because there does not appear to be consensus on definitions for these words, particularly for the word information, an attempt will be made to clarify their meanings solely for the purpose of this research project and for the context in which information will be viewed.

6.2.1 Data Processed …

Within the Information Systems and Information Technology (IS/IT) arena, it is accepted that *input (data) – process – output (information)* is agreed upon (O'Brien, 2000; Oz, 2002). The word data is the plural of the Latin word *datum*, though data commonly represents both singular and plural forms. According to

O'Brien (2000, p.27), the word data refers to *"raw facts or observations, typically about physical phenomena or business transactions"*. Oz (2002, p.8) clarifies the word information within the IS/IT context and states: *"Information can be raw data or data manipulated through tabulation, addition, subtraction, division, or any other operation that leads to greater understanding of a situation"*.

Figure 6.1, *Information in Context* is the accepted paradigm of how information is viewed for this research project even though some alternate views will be discussed. Figure 6.1 is also known as Venkatraman's DIKAR model (Data, Information, Knowledge, Action, Results). The perception that *Data processed* becomes information and *Information interpreted* becomes knowledge is the generally accepted view within the IS/IT field; then importantly *decisions*, based on knowledge, *direct* the company and ultimately determine the company's business results. As shown in Figure 6.1, there is a counter flow starting with the company's external environment that feeds back until it is captured as data and is again prepared for processing.

An example of Figure 6.1, applied to stock in a company, could start with the data collected regarding the amount of stock stored at warehouses. The pure numbers by themselves are data. When processed (totalled), it becomes information. Based on this information, interpreting the value of the stock becomes knowledge as to the value of the assets stored. Depending on the value of the assets, decisions can be made to increase sales/stock or for example, apply for financial loans (bank overdraft), using the stock as collateral for these loans. As mentioned, this can help determine the company's actions and affects the overall business results. This linear approach clearly illustrates the importance of having *accurate* and *reliable* figures (data) at the start of the process.

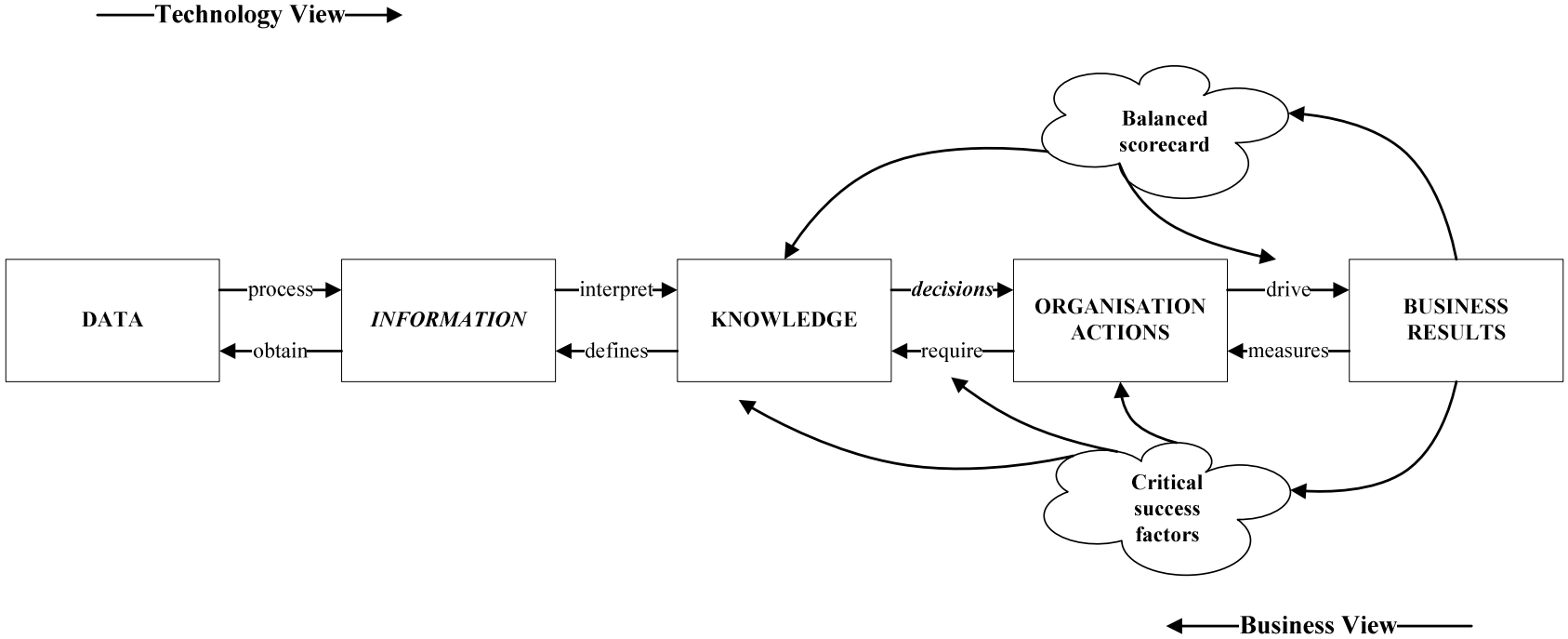

Figure 6.1: Information in Context (by N. Venkatraman, 1996, in Ward & Peppard, 2002, pg 207)

6.2.2 What Constitutes Information?

In an attempt to describe what constitutes *information,* Machlup and Mansfield reviewed and edited numerous articles on the subject. This they did from various perspectives covering many disciplines. Their project was to *"analyze the logical and pragmatic relations among the disciplines and subject areas that are centered on information"* (1983, p.3). This extensive book, which is often quoted, almost appears contradictory and confusing (depending which disciplines one subscribes to); however, this also highlights that one can find references and quotations supporting the different stances on the subject.

It is emphasised that the discipline, *Information Theory*, is at times referred to by alternate names within the scientific domain, such as: *"mathematical theory of communication, communication theory, coding theory, signal-transmission theory, and mathematical theory of information measurement*" (Machlup & Mansfield, 1983, p.47). They continue and discuss whether Information Theory is chiefly about *information* or *communication* or about *signals.* Later they comment that the word *Communication* is a possible alternative for the word *Information.* However, they clarify that the words also have other meanings (Machlup & Mansfield, 1983).

Another view to consider is Mesarovic's (1983, p.569), who contends that information cannot be defined without reference to the goal-seeking behaviour of a system (in harmony with systems theory). He explains: *"A system is goal-seeking if its behaviour can be best described with reference to the pursuance of a given goal"*. An example he uses to illustrate his point is that a system-dynamic approach would describe this in terms of the car's acceleration and speed, that is, as a physical system. Mesarovic continues that a goal-seeking description would require that *"the driver inside the car be identified and the moving point on the line representing the car on a highway be represented in terms of the strategy the driver uses in steering the vehicle along the road"*.

To summarise Mesarovic's view (1983), a goal seeking description, therefore requires a description of a goal, a description of a strategy and the description of the environmental conditions in which the strategy is being pursued. Mesarovic (1983, p.570) argues that the concept of information is *"much richer"* than most perceive it to be and therefore he makes a bold statement and an important link that he *"would actually equate systems theory with information theory in an appropriately wider sense"*. Additionally, he extends the disciplines and states that; *"information theory and systems theory are one and the same"*. This last statement of his has received some criticism.

Machlup (1983, p.642) contends that any other meanings for the word *information* other than the two he lists below are analogies, metaphors or concoctions, first being *"the telling of something"* and secondly *"that which is being told"*. He expounds on this and elaborates that there are many different methods however: *"Information is a flow of messages"* (1983, p.643). Machlup does point out, which has already been established, that it is not a requirement *"that information be correct and knowledge be true"*. Chapter Two on corporate governance argued that information can be misleading, incorrect and even false or fabricated.

Machlup (1983, p.645) also emphasises that information involves at least two parties, *"One who tells (by speaking, writing, imprinting, pointing, signalling) and one who listens, reads, watches"*. This is essential as one considers the Stag Hunt (discussed in Chapter Three), in which the hunters send messages or signals in order to share information with each other as they conduct their hunt. Or to reiterate, the board of directors, sending messages or signals to the company stakeholders via the financial statements, are sharing information. This is in harmony with the view that Mesarovic and others subscribe to, which is that a system is goal-seeking provided it has a clear objective.

The following Table 6.1 is presented by Bovee (2004) as a non-exhaustive summary of the work presented by Machlup and Mansfield (1983). Bovee

(2004, p.11) states, *"the list details the implied specializations of the word 'information' that occurred in the literature without adjectival modification"*.

Table 6.1: Exclusionary Narrowing of the term 'Information' by Machlup and Mansfield (Bovee, 2004, p.11)

To be 'Information' something must…..
Be previously unknown
Be previously less assuredly known
Affect the recipient's knowledge stock or structure
Consist of raw, uninterpreted data
Be useful in some way
Be used in decision making
Bear on contemplated, considered or taken actions
Reduce uncertainty
Help identify contextual meaning of words in sentences
Exclude some alternatives to what is predicted in a statement
Change some belief(s)

The fourth line from the top in the table (which has been *italicised – "consist of raw, uninterpreted data"*) is in conflict to Figure 6.1. Machlup (1983, p.648) proceeds and states that: *"There is no need to establish either a hierarchy or a temporal sequence in discussing data and information. Apart from computer systems the two words may be equivalents"*. As noted, not everyone agrees with the linear approach that data processed becomes information and information enhanced by experience becomes knowledge. This became clear when conducting the literature survey. Some researchers claim that knowledge is also information depending on the context.

Firestone and McElroy (2003) attempt to clarify distinctions between data, information, and knowledge in the context of their research (their focus is Knowledge Management). They describe *data* as (2003, p.17) *"the value of an*

observable, measurable, or calculable attribute". In addition, they state that (2003, p.18) *"information is frequently data extracted, filtered or formatted in some way"*. However, Firestone and McElroy also subscribe to the school that data, information and knowledge do not need to be treated as a hierarchy or in a linear fashion. In spite of this, they share the same view as the IS/IT field as to what constitutes data, information and knowledge, just not necessarily the order in which they are produced.

In contrast to the above paragraph however, and in agreement with Figure 6.1, the Barabba-Haeckel Framework is discussed by Barquin (2000). As with Figure 6.1, the focus of this chapter is not on the latter part of the framework, but the first half. Barquin describes the framework as a continuum that starts with data and goes through stages until it is eventually wisdom. Figure 6.2 is used to illustrate this framework.

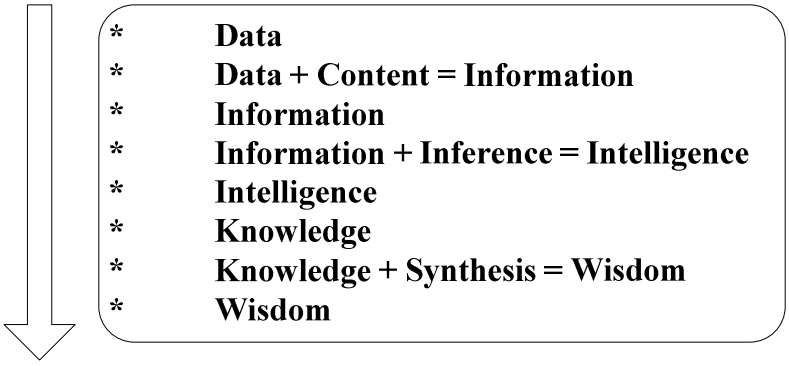

Figure 6.2: The Barabba-Haeckel Framework (Barquin, 2000)

English's (1999) model of the relationship between data, information, knowledge and wisdom is in harmony with both Figures 6.1 and 6.2. Accordingly English explains that useable data allows meaning to be extracted from it, resulting in information. This information in context, allows one to determine its significance, which results in knowledge. The action based on knowledge results in wisdom.

Nevertheless, it is not the focus of this chapter to attempt to provide a 'perfect' understanding of the various views on what constitutes data, *information* and knowledge as this is beyond the scope of this research project. The purpose is merely to illustrate that there are different views on the subject; however, there is agreement that data does influence and have an impact on information. This thesis argues that information does influence the decisions taken by decision makers and the results of these decisions affect the company and its performance (as shown in Figure 6.1).

Tuomi (1999) adds that when meaningful information is used in context, it becomes knowledge and is used to *make predictions*. In Chapter Three (Section 3.2.1), it was discussed that positive predictions about future actions between parties is a prerequisite to uncertainty reduction. As noted before, predictability and uncertainty reduction lead naturally to the development of trust.

6.2.3 Information and Communication

It is beneficial to clearly link the information found within a company's financial statements to Communication Theory. Taking this view, which some may argue is conceptual and has not been proven mathematically, is however in line with Mesarovic's view described in the previous section. This is done in order to help reduce uncertainty between parties, which is important to emphasise as uncertainty affects behaviour. The financial statements are viewed as a means of communication between the board of directors with the various company stakeholders.

Shannon and Weaver (1949) were referred to at the beginning of this thesis when introducing communication and technology, specifically the sending and receiving of *messages*. The work of these researchers has formed the basis of many other research projects and papers. However, Shannon's previous work in 1948, which formed the core of the 1949 publication, is also of interest because it addresses the amount of uncertainty reduction that can occur when one receives a message from a *finite* set of possible messages. As noted, this form of

communication could be likened to the hunters sending messages to each other during their hunt as discussed in the Stag Hunt/Assurance Game in Chapter Three (Section 3.3.3). In addition, it is comparable to the directors sending messages to the various company stakeholders via financial statements as to the financial condition of the company.

Shannon's theorem included a proposed graph and formulas arguing that the maximum possible *uncertainty reduction* or *entropy* occurs when both symbols (one representing uncertainty and one entropy) are equiprobable. In other words, when a system has two possible outcomes, the uncertainty or entropy in the system is maximised when both outcomes have the same probability. Information Entropy or Shannon's Entropy, which it is occasionally called, is an important point when one researches the *'condition'* of information. However, for this thesis it is not necessary to duplicate too much of Shannon's work, but rather to focus on the work he contributed in the area of uncertainty reduction associated with the receiving of messages.

Figure 6.3 is Shannon's diagram illustrating a general communication system. Even though Shannon referred to a technical system, proving his theory by using a logarithmic approach, the principles he proved are applicable to this research project. As noted previously, there is a school that argues, for example, that Shannon's notion of information refers only to the capacity for transmission. However, applying information as described in Shannon's work together with Mesarovic's research provides a wider view when one considers a goal-seeking system.

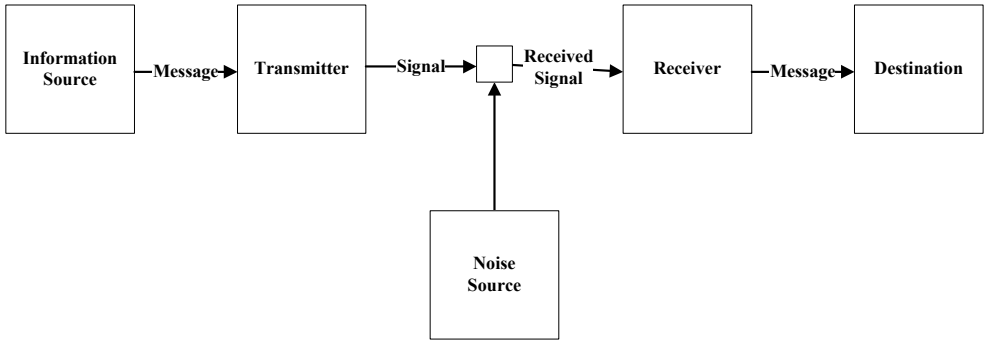

Figure 6.3: Schematic Diagram of a General Communication System
(Shannon, 1948)

Shannon explains the parts of his diagram as follows: The *Information Source* produces a message or a sequence of messages to be communicated to the receiver. Then the *Transmitter* operates on the message in some way so as to produce a signal suitable for transmission over the channel. The *Channel* is merely the medium used to transmit the signal from the transmitter to the receiver. The *Receiver* ordinarily performs the inverse operation of that done by the transmitter, reconstructing the message from the signal. Finally, the *Destination* is the person for whom the message is intended. Shannon also discusses the *"effect of noise in the channel"*.

When one considers Figure 6.3 and contemplates either the Stag Hunt/Assurance Game or the board of directors sending messages via the financial statements (*the channel*), one can observe the ease at which the *"noise in the channel"* can corrupt the message (either intentional or unintentional errors within the financial statements). The *information source* is the company producing a *message* which is *transmitted* via financial statements to the *receiver.* The receiver could be any of the company stakeholders relying on the *message* found within the company financial statements.

Shannon proposes a solution to help counteract the effect of the noise in the channel. This is illustrated in Figure 6.4 where *"an observer who can see both*

what is sent and what is recovered (with errors due to noise)" is put in place. *"This observer notes the errors in the recovered message and transmits the data to the receiving point over a 'correction channel' to enable the receiver to correct the errors"* (1948, p.21).

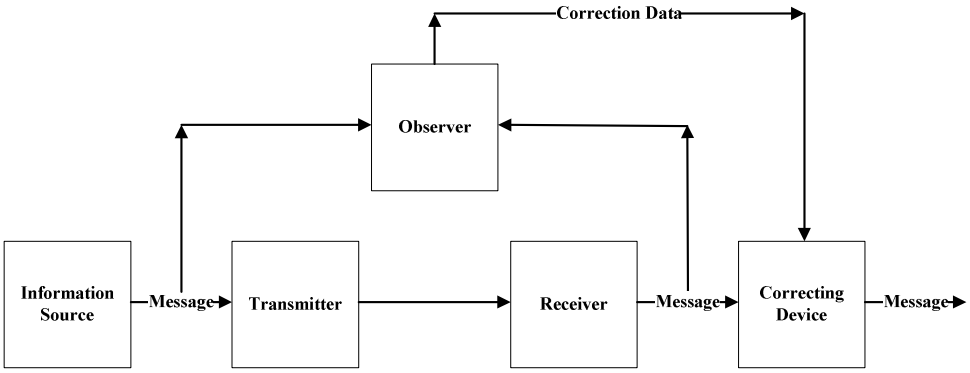

Figure 6.4: Schematic Diagram of a Correction System (Shannon, 1948)

Such an observer, within the context of this research project, could be an auditor. It is important to note the change in the process (Figure 6.3 versus Figure 6.4) which allows the *Observer* access to the message, both at the Information Source and after the Receiver has received the message, to 'make a comparison' and report on the *condition* of the information. The *Correcting Device* can be likened to a corrective control or controls that ensure the message is a *faithful presentation* of the original message. This leads to the next section which discusses information *quality*.

6.3 THE CONCEPT OF INFORMATION QUALITY

Information is an important commodity and it is not difficult to reach a point where one enters a stage of information overload due to the abundance of this commodity. Having said that, the management of information is a specialised discipline and decisions are based on the information available. The decisions made are affected by the quality of the information on which the decisions are based (this was noted in Chapter Two, Section 2.2.3). Poor quality information

has contributed to lost productivity, failed companies and low consumer confidence (English, 1999; Wang & Strong, 1996). Poor quality information has also caused political controversy and high-profile disasters (Fisher & Kingma, 2001).

6.3.1 Quality Decisions

As decisions are affected by information, if the information lacks quality, this has a natural effect on the outcomes of the decisions and hence, the decisions ultimately lack quality. To ensure fact based decision-making, one would require assurances as to the condition of the information when the decisions are made. If decisions are made in real-time, based on real-time information, one would require real-time assurances. This is discussed in more detail in Chapters Seven and Eight.

However, it is important to take note that *"high quality decisions are expected to lead to more productive actions, quicker problem solving, and better organizational performance"* (Jung, 2004, p.166). In other words, a director can perform his or her duties more effectively and the principles of good governance can be applied. Jung continues and points out that to make high quality decisions, it is crucial to have access to information that is relevant and complete on which to base decisions rather than just having an enormous quantity of information. Consequently, companies where decision makers experience information quality problems, can end up taking unnecessary risks by accepting impractical ideas and making errors in interpretation, or ignoring important ideas (Jung, 2004).

Since risk is intrinsic to governance, a board of directors needs to ensure that their risks are mitigated to an acceptable level. This of course includes the risks associated with their decisions based on corporate financial information. Due to many boards failing in this duty and the increase in corporate debacles (as noted in Chapter Two), many influential 'codes' have been imposed on companies

enforcing that the information held within the company's information systems receives a higher priority.

Compliance to the Sarbanes-Oxley Act, Basel II Accord and other 'codes' calls for heightened internal controls over the financial processes, implying an increased focus on IS/IT to provide a secure and auditable infrastructure. The current quality control standards, for example ISO 9001, concentrate on quantitative controls. These place the emphasis for process development on the controlling, documenting and monitoring rather than the qualitative aspect of the work performed. The 'imposed codes' are watershed regulations for companies as they mandate a rigorously controlled environment in which information systems operate and a high standard of *quality information* is created, documented and stored (control was discussed in Chapter Four).

Accordingly, the philosophy of Total Quality Management (TQM) is that continuous improvement must be applied to all quality standards. Thus, if one considers risk management, data and information quality standards are aspects to be considered. The reason is that poor information can cause a company to miss its strategic objectives due to the decisions based on that information. The company's reputation and the director's credibility could be severely damaged by the results of decisions based on poor quality information.

6.3.2 Data Quality – the Foundation of Information Quality

Ward and Peppard (2002) succinctly point out that the challenge companies have is to ensure that information is of the highest quality possible. As noted, information quality in part is based on data quality. By studying Wang et al.'s research, as Wang appears to be one of the foremost researchers in the IS data and information quality fields, it became evident that the attributes or dimensions of data and/or information *quality* are not agreed upon. However, a model of what is perceived to be the dimensions (as named by Wang) of data quality is proposed by Wang and Strong (1996) and illustrated in Table 6.2.

Table 6.2: Data Quality Categories and Dimensions (Wang & Strong, 1996)

Data Quality Category	Data Quality Dimensions
Intrinsic DQ	Accuracy, Objectivity, Believability, Reputation
Accessibility DQ	Accessibility, Access security
Contextual DQ	Relevancy, Value-Added, Timeliness, Completeness, Amount of data
Representational DQ	Interpretability, Ease of understanding, Concise representation, Consistent representation

Even though Table 6.2 assists in clarifying what constitutes data quality, it is inconclusive as there appear to be many different views on this topic. Furthermore, to gain a 'clearer' understanding of the attributes of information quality a table (Table 6.3) summarising the work of seven research groups was created for comparison. This table is evidence that there appears to be disagreement on what constitutes information quality or at least disagreement on the use of words and terminology. Wang and Strong clearly present the largest number of attributes with both Bovee, Srivastava and Mak (2003) and ITGI (2004) with only four each.

Table 6.3: Terms used to Describe the Attributes of Information Quality

Information Quality Attributes	Ward & Peppard (2002)	Wang & Strong (1996)	Eckerson (2002)	Bovee et al. (2003)	Wand & Wang (1996)	ITGI (2004)	IASB & FASB (2006)
Accessibility		**X**	**X**	**X**			
Accuracy	**X**	**X**	**X**		**X**		
Appropriateness	**X**						
Believability		**X**					
Comparability							**X**
Completeness	**X**	**X**	**X**		**X**		
Concise		**X**					
Confidence	**X**						
Consistency		**X**	**X**		**X**		
Flexibility					**X**		
Integrity			**X**	**X**		**X**	
Interpretability		**X**		**X**			
Materiality							**X**
Objectivity		**X**					
Relevance		**X**		**X**		**X**	**X**
Reliability	**X**				**X**	**X**	**X**
Security		**X**					
Timeliness	**X**	**X**			**X**		
Understandability							**X**
Usability						**X**	
Validity			**X**				
Value-added		**X**					

When one studies this table it becomes clearer that the words have semantic meanings and this appears to cause confusion. From observation, it does not appear that these researchers disagree in any major way as to what attributes constitute information quality. It is more the use of the words they have chosen and their terminology in general.

For example, the words *accuracy* and *integrity,* which are recognised as crucial attributes of information quality, are used inconsistently. Only four of the seven

research groups list accuracy as an attribute as shown in Table 6.3. However, integrity is listed by three of the seven and *one* research group refers to both accuracy *(correctness, exactness, precision, truth)* and integrity *(truth, reliability, completeness, wholeness).* There is a subtle difference in the meanings of these two words, but one can see how they are at times used interchangeably.

Wand and Wang (1996) conducted research on what constituted information quality and produced a table listing their results. *Accuracy* was cited more than any other attribute in importance. However, interestingly their table is called *"Notable data quality dimensions"* (1996, p.92) not *information* dimensions. Yet they conducted research as to what constitutes information quality, but substituted the word data for information when naming their table? Additionally, they did add that *"there is no exact definition for accuracy"* (1996, p.93). This may highlight why there are so many different terms used to describe information quality.

To continue with the example of accuracy, Bovee et al. (2003) emphasise that accurate information generally relates to whether or not the information corresponds sufficiently with its tangible or conceptual real world. If one accepts Bovee et al.s definition of accuracy, one can see why some researchers have used the word integrity in the place of accuracy.

An interesting output of Redman's (1998) research is that he argues a typical impact caused by inaccurate data is that of *"increased organizational mistrust"* (1998, p.82). Even though Wang and Strong (1996, p.32) do not refer directly to trust or mistrust in their table, they do refer to *reputation* along with *accuracy* as dimensions of Intrinsic DQ (Table 6.2). When defining reputation they state that it is *"the extent to which data are trusted or highly regarded in terms of their source or content"*.

Redman's research (1998) also claims that 1%-5% of all data fields are erroneous. This is supported by a survey conducted in the USA in 2003 of

accredited medical records managers, who found that 4%-7% of their financial records had significant errors. Accordingly, these either resulted in over or under reimbursements of billing claims (Boritz, 2005, p.261).

This section, including Table 6.3, clearly illustrates that there is not agreement among researchers on the use of words and terminology describing the attributes (or dimensions) of data and information quality. However, regardless of the words used to describe information quality, Boritz (2005, p.262) highlights an important point that *"it would be hard to imagine information having quality in the absence of integrity"*. This leads to the next section which specifically focuses on information integrity.

6.4 THE INFORMATION QUALITY ATTRIBUTE OF INTEGRITY

Boritz (2005) contends that information integrity is not an isolated attribute, but draws on several other attributes (or as he refers to them – concepts). Boritz assisted the ITGI (2004) in one of the most extensive studies conducted in an attempt to clarify the understanding of information integrity. As noted in Table 6.3 and Figure 6.6, the IT Governance Institute (ITGI) presents four attributes *(reliability, relevance, usability, integrity)* of information quality. This research project subscribes to the ITGI view of information quality which appears holistic and thorough.

6.4.1 Firstly the Attributes of Relevance, Usability and Reliability

It is important to note that information quality is dependent on all four attributes. However, as noted the 'Achilles heel' is the attribute of integrity. For how could the information have *relevance*, *usability* and be *reliable* if it lacks *integrity*? Nonetheless, it is also important to note that the remaining three attributes overlap and complement each other when determining if one has quality information. This is shown in Figure 6.5. Additionally this figure shows the sub-attributes of these three attributes and emphasises that these are not mutually exclusive, but complement and contribute to each other (ITGI, 2004).

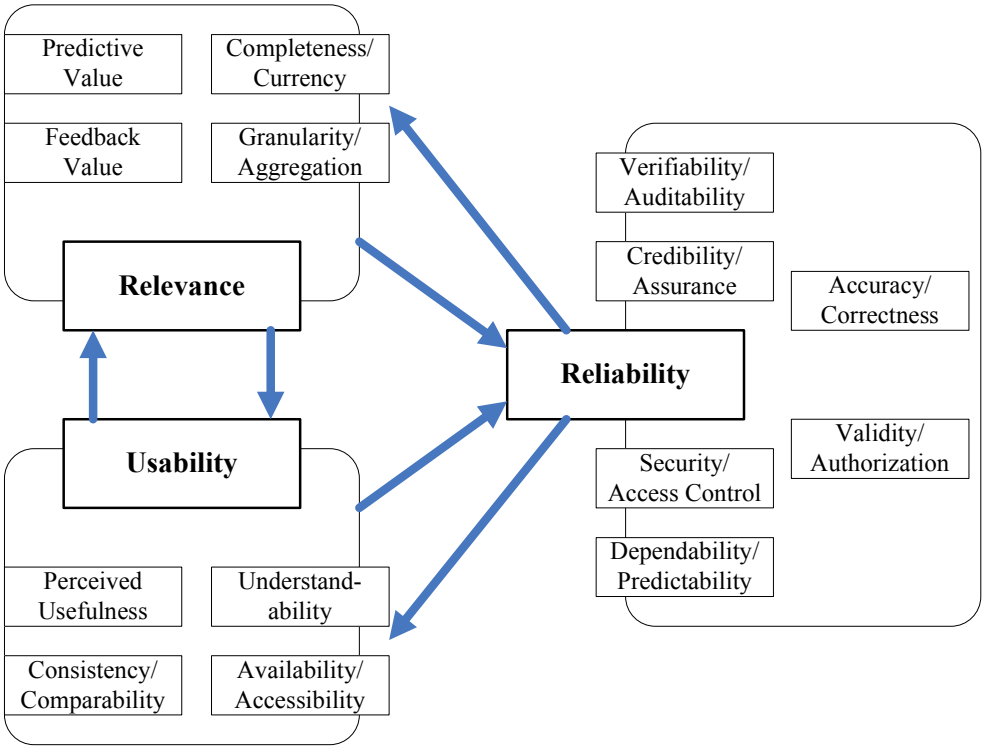

Figure 6.5: Relationship among Relevance, Usability and Reliability
(ITGI, 2004, p.21)

Brief explanations or definitions are provided for *relevance*, *usability* and *reliability*.

- *Relevance* is referred to by four of the seven research groups in Table 6.3. According to the ITGI (2004, p.16), it is *"the information's capacity to make a difference that identifies it as relevant to a decision"*. However, the ITGI points out that it is the *"theoretical capacity"* of the information that contributes to the objective of information production.
- *Usability* or, as some have referred to it, usefulness, reflects the users' *"perceptions of the practical value of information they believe will help them in completing their work"* (ITGI, 2004, p.18).

- *Reliability* is also referred to by four of the seven research groups in Table 6.3. Accordingly, the ITGI (2004, p.20) explains that reliability *"reflects the signal-to-noise value of information used in decision-oriented systems"*. Or expounded on, *"the less uncertainty and risk surrounding information"* the more reliable the information.

Interestingly, the International Accounting Standards Board (IASB) and the Financial Accounting Standards Board (FASB is based in the USA) advocate that the word *reliability* is replaced with the words *"faithful representation",* as in their view the word reliability is widely misinterpreted (FASB, June 1, 2005; IASB & FASB, May 16, 2006).

6.4.2 Understanding Integrity and its Sub-attributes

According to the ITGI (2004), the external oval in Figure 6.6 encompasses information and the three circles within the oval illustrate attributes of information quality (as illustrated in Figure 6.5 which provides a more in-depth view of the three circles). The fourth attribute, which is the central oval, represents *Information Integrity*. The strategic placement of this oval illustrates the significance of integrity to the information's value.

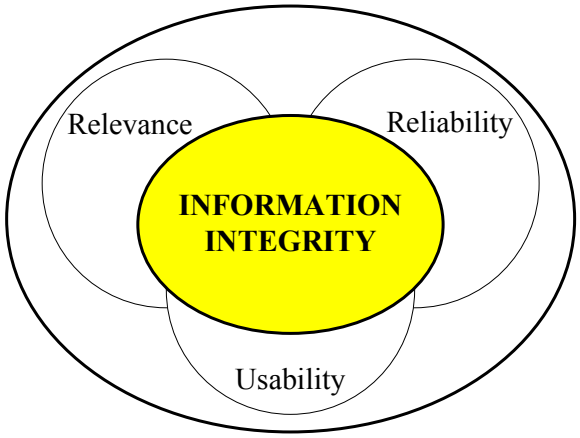

Figure 6.6: Information Integrity (ITGI, 2004, p.3)

As mentioned, it is important to observe the positioning of the information integrity oval in relation to the three circles (relevance, usability and reliability), thereby overlapping and incorporating elements of all three. It is also worth noting that information integrity is a narrower concept than information quality; although, it is a broader concept than data integrity (ITGI, 2004).

In the same manner that relevance, usability and reliability have sub-attributes, so does integrity. As with the attributes of information quality there also appears to be disagreement among researchers as to what constitutes information integrity, or more specifically what are the sub-attributes of information integrity.

However, information has its integrity if the accuracy, completeness, timeliness, validity and processing methods are safeguarded (ITGI, 2004; Carlson, 2001; NIST 800-12 Handbook, 1995). According to the IT Governance Institute (ITGI, 2004, p.22) integrity means unimpaired or unmarred condition. Applied to information, *"integrity is the representational faithfulness of the information to the condition or subject matter being represented by the information"*.

Figure 6.7 is used to illustrate the sub-attributes of information integrity according to the ITGI (2004) and Bovee et al. (2003). These two research groups were chosen because their research appears extensive and thorough within this research domain. In addition their research is more current than most others.

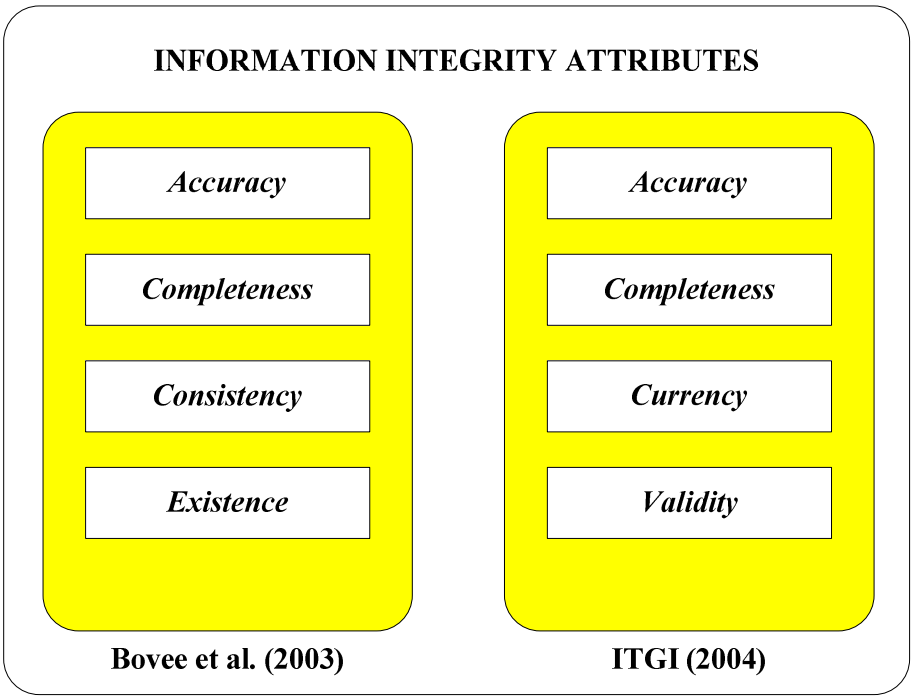

Figure 6.7: Information Integrity Attributes

Bovee et al.'s (2003) research produced four attributes of information quality and related them to the process of *how* information is created (see Table 6.3). Three of these attributes they described as *extrinsic* (*immaterial, insignificant, nonessential*) in nature - these are accessibility, interpretability and relevance. However the fourth attribute, *Integrity*, they claimed was *intrinsic* (*material, central, essential*) in nature when related to the process of how information is created.

Bovee et al. (2003) define the four sub-attributes of *integrity,* which is intrinsic to how information is made, this way:

- *Accuracy* – This information conforms to the real-world or conceptual items of interest to the user. It is typically considered to be error free.
- *Completeness* – Refers to having all required parts or having enough information for decision-making.

- *Consistency* – Requires that multiple recordings of the values for any of the attributes be consistent across time and space. To be consistent these values must be the same in all cases.
- *Existence* – This is an important intrinsic element of information used in auditing. If one needs to validate information, Bovee et al. (2003) claim that the information would need to meet any tests of existence that there are no false or redundant entities, fields or values.

The ITGI (2004) define the four sub-attributes of *integrity* this way:

- *Accuracy* – The information is a faithful representation of events.
- *Completeness – "All information necessary to reflect business activity in accordance with established business rules is captured, processed, stored and reported"* (ITGI, 2004, p.29).
- *Currency* – The information is current and timely and within preset definitions of the duration of time in an information period.
- *Validity* – The information would be considered valid if it is authentic, not duplicated inappropriately, nonrepudiable, and in accordance with specific business rules that define relationships among information items, governing form, content, function, time, source and destination.

The first two sub-attributes, *accuracy* and *completeness*, are the same for both the ITGI and Bovee et al. even if defined slightly differently. However, it appears as if both research groups are saying the same thing. The third sub-attribute, *consistency* or *currency,* has overlapping qualities but a slightly different focus. The fourth sub-attribute, *existence* or *validity,* is not defined too dissimilarly. This once again highlights the semantic meanings of the words and the terminology favoured by the particular researchers.

Interestingly, a few of the other researchers in Table 6.3 listed some of these 'sub'-attributes or used similar words when describing information quality attributes. Nevertheless, Bovee et al. (2003), Boritz (2005) and the ITGI (2004)

all emphasise the significance of the attribute of information integrity. Bovee et al. (2003, p.32) define the integrity of information as being *"satisfactory free from defects or flaws"*. This sums it up and leads to the next section that data integrity alone is insufficient because one also requires system integrity.

6.4.3 Data Integrity + System Integrity = Information Integrity

Figure 6.8 graphically depicts the process of how information integrity is achieved. This demonstrates that to have information integrity both the *data* and the *system* (including IT infrastructure) need to have integrity. As discussed, data is considered to be the raw material used to create a finished product ready for use, i.e. information. It is important to note that besides the *data*, information integrity is dependent on *system* integrity. In other words, information integrity can be no better than the integrity of the system processing the data or information, although it can be worse (ITGI, 2004; Woodroof & Searcy, 2001).

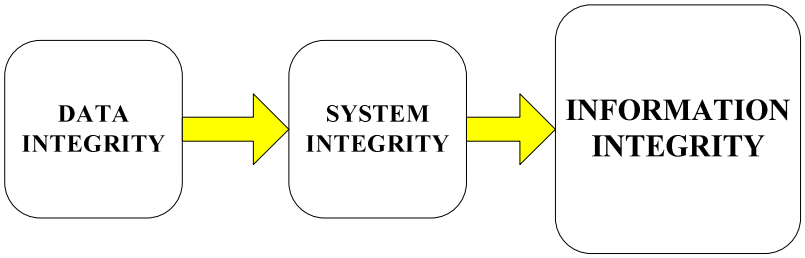

Figure 6.8: The Requirements of Information Integrity

A system demonstrates processing integrity if *"its outputs fully and fairly reflect its inputs, and its processes are complete, timely, authorized and accurate"* (ITGI, 2004, p.5). To emphasise the two aspects (Figure 6.8), a system may have integrity, but if the data it processes lacks integrity at the time the system receives it, then the data can continue to lack integrity when it is transferred to its destination or transformed into information. Transmission integrity is therefore not treated as a separate element, but part of system integrity.

The following is a costly example of a processing error and its consequences when information lacks integrity. Due to bank error in the currency exchange rate, an Australian was able to purchase Sri Lankan Rupees for AUS $104 500 and then sell them to another bank the next day for AUS $440 258. The original bank's computer displayed the central Pacific Franc rate in the Rupee position. Because of the circumstances surrounding the bank's error, a judge ruled that the Australian man had acted without intended fraud and could keep his windfall of AUS $335 758 (ITGI, 2004, p.7).

Another discomforting example (of which this is just one of many) is Fannie Mae's third quarter 2003 FAS 149 spreadsheet based calculations understating the value of the mortgage loan commitments by US $1.3 billion. Fannie Mae is a US company providing financial services, specifically mortgages. Fannie Mae attributed this to *"human error"* (Boritz, 2005, p.261).

These examples draw attention to the fact that both the data entering the system and the system processing the data needs to have integrity. Figure 6.9 is based on Figure 6.1 (Information in Context) and more detail is provided on how integrity is integrated into the *technology view* of decision-making. The results of these decisions determine the business results which will have an effect on predictability and uncertainty reduction. When uncertainty is reduced to an acceptable level, trust will grow and the overall confidence will be increased in the produced results.

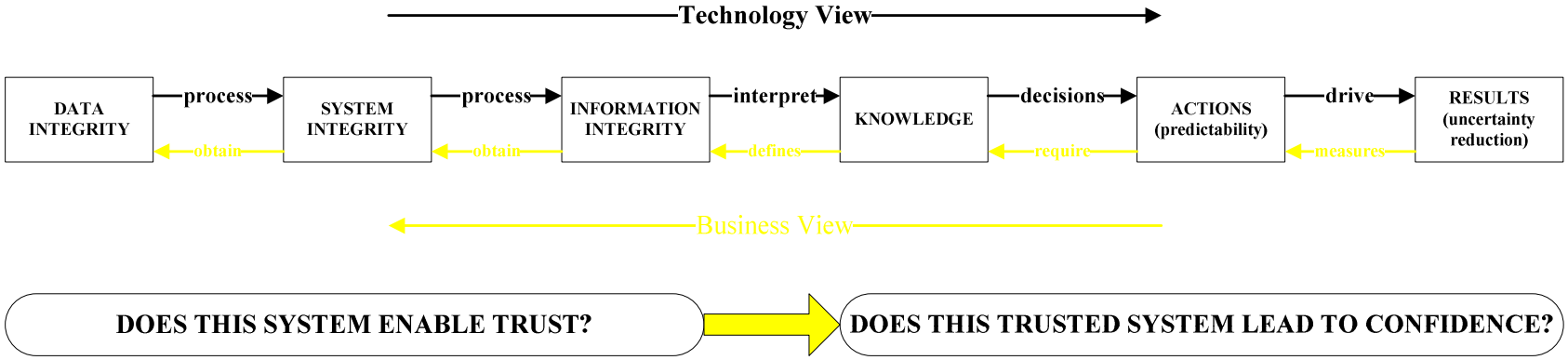

Figure 6.9: Information Integrity in Context

It therefore becomes imperative to have controls in place to ensure both data and system integrity (as illustrated in Figure 6.9). As discussed in Chapter Five, a process is also needed for validating these controls and reporting on their status, thereby providing assurances as to their condition. This stresses the importance of risk management, especially information security, which subsequently plays an important function ensuring information integrity. System integrity, even though only briefly discussed in this chapter, is referred to in several other chapters of this thesis and will be discussed in more detail in the following chapters.

6.5. CONCLUSION

This chapter discussed the linear sequence in which data processed becomes information and information interpreted becomes knowledge. It stresses that decisions are based on knowledge and determine the company's business results. This was followed by a rich debate clarifying the attributes of *information quality* and the attributes of *information integrity* for the context of this thesis.

This chapter proposes that information quality is essential to a company's success. However, the information cannot have quality if it does not have integrity. For the information to have integrity, both the *data* and the *system* need to have integrity. To have system integrity, a company needs to have a sound system of internal controls with IT controls at its core. The reason for this is that information is often found in electronic formats within the company's business processes. The controls need to limit uncertainty and the risks need to be mitigated to an acceptable level. This is one component of information integrity; the other is data integrity.

The auditors have several tools and techniques that assist them in determining whether the data has its integrity or not (as discussed in Chapter Five). Continuous auditing is proposed as the way forward whereby assurances can be

provided in real-time, thus providing current information with more credibility for decision-making. This will be discussed in more detail in the following two chapters.

Finally, it is important to note that any directors practising good governance would need to ensure that the information within their company's financial statements has its integrity intact. This would lead towards building trust and restoring investor confidence between the various company stakeholders and the board of directors.

Chapter 7

THE CONCEPT OF CONTINUOUS AUDITING

"If you can't describe what you are doing as a process, you don't know what you're doing."
- William Edwards Deming, (management consultant, 1900-1993)

7.1 INTRODUCTION

As discussed in the previous chapter, information integrity within financial reports is crucial to building trust. Therefore, continuous auditing is proposed as a method of verifying the information's integrity in real-time and on a continuous basis. This is in line with the Sarbanes-Oxley Act calling for reporting to be done on a *"rapid and current basis",* where this refers not only to near real-time reporting, but also to near real-time assurances (Alles et al., 2005). Additionally, Alan Anderson (AICPA, 2002), Senior Vice President of AICPA, describes the business-reporting model of the future as *"online, real-time disclosure"*. He continues by pointing out that users want *"data on demand"* as well as more relevant and up to the minute information to assist in better decision-making.

With the integrity of the information within financial statements in question and the shift towards more rapid financial reporting, the auditing profession has had to find new ways of verifying information in these reports. Therefore, the need for timely and ongoing assurances regarding the effectiveness of risk management and internal control systems is critical.

In this chapter, it is essential to differentiate between *continuous monitoring, continuous auditing* and *continuous assurances*. Firstly, continuous monitoring is discussed followed by an in-depth examination of continuous auditing. Finally, continuous assurances is addressed as it is the auditors who will provide the continuous assurances that management have a successful monitoring system in place for both their internal control system and risk management practices over financial processes.

7.2 CONTINUOUS MONITORING

Continuous monitoring is a management mechanism or function whereby senior management monitors and assesses the control and disclosure environment within the company on a continuous basis (Flowerday & Von Solms, 2005a; GTAG1, 2005; Warren & Parker, 2003). This view is in line with the COSO view that recommends that management fulfils the monitoring role of the internal controls on a continuous basis and identifies, assesses and determines the company's exposure and management's response to risk. Krell (2004) adds that the senior financial managers should identify high-risk areas and then prioritise their business processes according to risk areas or factors to be monitored within the financial processes.

Thus, the recommended process for continuous monitoring is that it should be instituted by management and where possible, should be supported by technology, which provides feedback to management on whether the controls surrounding the business processes are effective and efficient. This should be on an ongoing basis as technologies, for example, intrusion detection software, continually monitor network traffic for evidence that other protective controls, such as firewalls and virus protection, have been breached (GTAG1, 2005).

The monitoring process should identify weaknesses and 'flag' anomalies (or as auditors refer to them, exceptions) for immediate follow-up. This is illustrated in Figure 5.1 (Flowerday & Von Solms, 2005a) which is reinserted in this chapter

as Figure 7.1 due to its importance. This high-level illustration effectively demonstrates the responsibilities and reporting lines for *monitoring* and *auditing*.

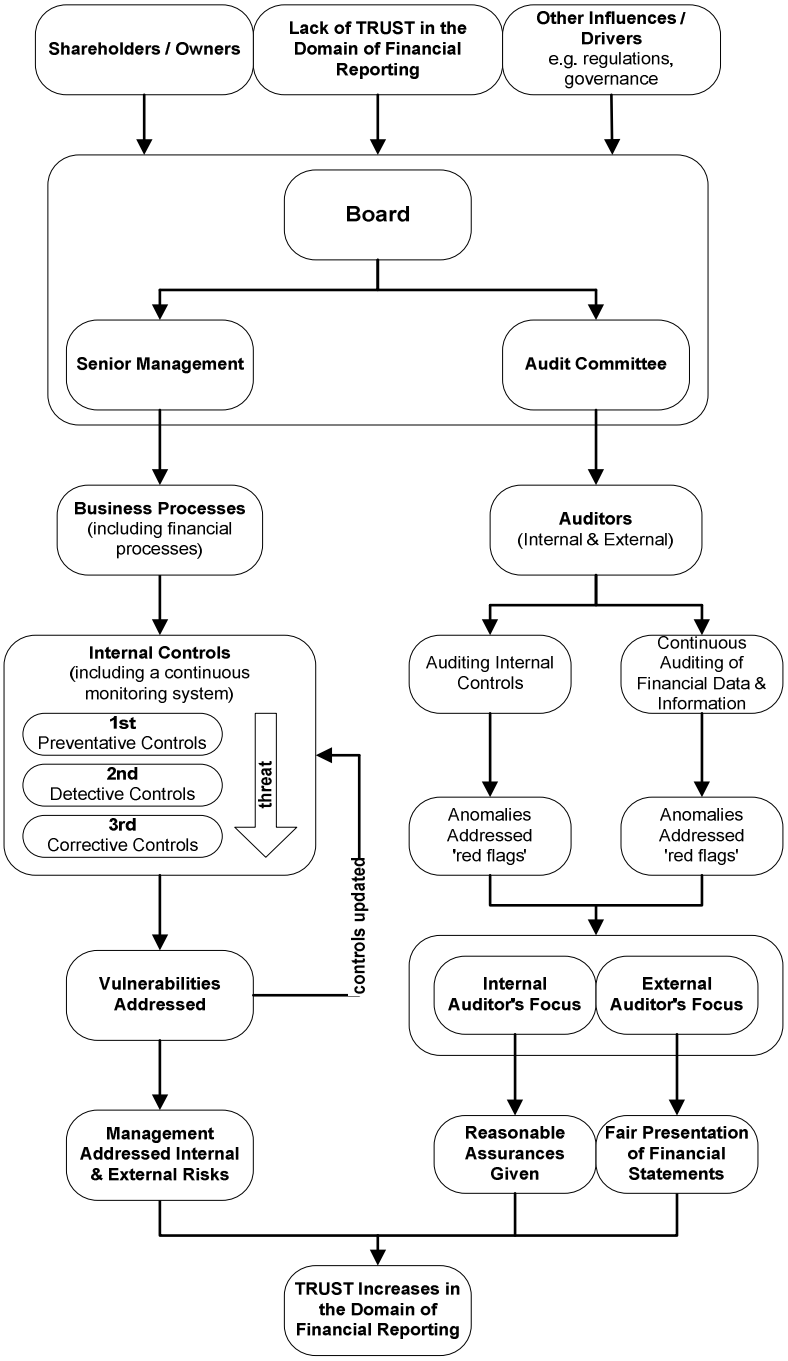

Figure 7.1: High-level Flowchart Illustrating the Management and Audit Processes (Flowerday & Von Solms, 2005a)

Today, automated monitoring of business processes in real-time is becoming more widely accepted. This is especially true of large companies using company wide ERP systems where software vendors have made an attempt to provide companies with modules which assist with monitoring, for example, SAP-MIC (Management Internal Control module). In addition, there are guidelines, such as CobiT, that are provided by organisations such as ISACA and which assist management with this responsibility.

The use of 'desktop dashboards or control charts' that report on high-level metrics such as Key Performance Indicators (KPIs), extract data from the monitoring infrastructure so that management receives current information and a degree of assurance that their system of controls is functioning as intended (Dull & Tegarden, 2004; Emery, 2004; Vasarhelyi, 2002). Emery (2004) proposes that the concept of KPIs should evolve into KRIs (Key Risk Indicators). The functionality of KPIs or KRIs is the same; however, the focus is different. Instead of focussing on financial or operational performance criteria, the KRI explores the same technique for measuring and controlling risk.

As noted by Emery (2004), the monitoring of internal controls and associated risk assists with compliance to Section 409 of the Sarbanes-Oxley Act. In addition, if the company is a bank, it would assist with compliance to the Basel II Accord that requires the monitoring and reporting of IT Risk. The Basel II Accord refers to this specific risk as IT Risk and positions it as a sub-section of Operational Risk.

Figure 7.2 illustrates the inverse relationship introduced by GTAG3 (2005) between the adequacy of management's monitoring and risk management activities and the extent to which auditors must perform detailed testing of controls and assessment of risk. GTAG3 (2005, p.9) contends that the amount of *"continuous auditing depends on the extent to which management has implemented continuous monitoring"*. They suggest that in the business

processes where management has not implemented continuous monitoring, auditors should apply detailed testing by employing continuous auditing techniques. The converse is proposed where management performs continuous monitoring on a comprehensive basis. Here, the audit activity effort can be reduced from what would otherwise be applied under continuous auditing. This is illustrated by the size of the arrows in Figure 7.2, by the narrow arrow representing the reduced auditing effort and the larger arrow representing the significant effort required by the auditors.

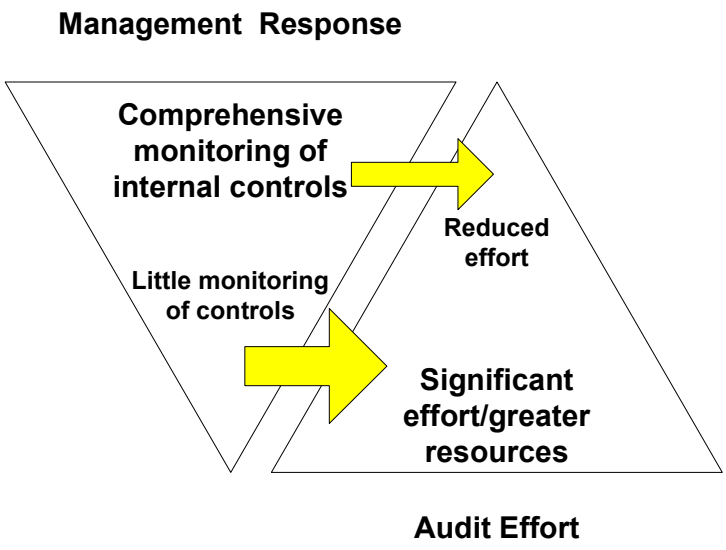

Figure 7.2: Inverse Relationship: Level of Effort Expended by Management and the Audit Activity (GTAG3, 2005, p.9).

It is important to highlight the point that Warren and Parker (2003) make that management should not be dependent on exceptions (anomalies) generated by auditors. Management should have their own monitoring processes in place to identify exceptions. They point out that if management does rely on the auditors to identify the exceptions, the auditing process becomes an integral part of the management process, which then qualifies as a classic control breakdown (as discussed in Chapter Two). This highlights the point that auditors need to

maintain their independence from management and report to the audit committee.

7.3 CONTINUOUS AUDITING (CA)

According to Krell (2004), continuous auditing is generally the responsibility of the internal audit department. He continues and emphasises that the internal audit department installs procedures that test both the business processes by scrutinising large volumes of individual transactions, and secondly, tests management's monitoring process which monitors systems that management uses.

In this thesis, the word *auditors* will refer to both internal and external auditors and will not distinguish between the two groups. There are researchers who contend that continuous auditing should be carried out by the internal audit department; however, other researchers argue that continuous auditing should include external auditors. This research project is not going to debate who should have the responsibility of continuous auditing, but rather demonstrate the importance of CA, what it is, and how it can possibly function in improving corporate governance and restoring investor confidence.

7.3.1 Motivation for the 'New' Business Process: Continuous Auditing

With the increased use of more sophisticated information systems in which the audit trail is not clear, auditors may be required to develop new processes, such as *continuous auditing,* for the testing and monitoring of the internal control environment and for conducting risk assessments. Thus, it appears that the auditing profession may be making a shift from historic *ex-post* audits to near real-time audits (Flowerday & Von Solms, 2005b). This is driven by the reality that decision makers need assurances that the real-time information they base their decisions on, is both accurate and reliable. Therefore, future real-time financial reporting is likely to necessitate continuous auditing.

While the auditing profession has long discussed this concept of continuous auditing, it has remained chiefly in the academic domain (Onions, 2003; Rezaee, Shabatoghlie, Elam, McMickle, 2002; Warren & Parker, 2003). However, there are strong drivers for this 'new' process and change in auditing methods. Marks (2001) points out that companies are rapidly installing new technologies that require auditors not only to understand them, but also to assess the risks associated with these technologies. As early as 1989 (Groomer & Murthy), it was recognised that information systems in companies were becoming increasingly complex and the traditional audit trail was disappearing. As a result, internal control and security have become critical concerns.

Evidence of the evaporation of the audit trail is that information today often exists in electronic form; hard copies or paper trails are disappearing relics of a previous era. Personal identifiers, i.e. signatures, are losing the paper and ink elements that have for centuries been the basis for *trust* and *controls* (Horton, et al., 2000). Flowerday and Von Solms (2005b) add that thus far, digital and electronic signatures are not yet as *trusted* as the paper and ink version, even though they are legally accepted in many countries. The reason they give is that it is difficult to prove who was using the machine/computer when the document was electronically signed.

The notion introduced by Vasarhelyi (2002) of the *"electronization of business",* where he points out the absorption and integration of technology into business processes, highlights the consequent changes this causes to business practices. This notion stresses the flow of electronic information within the company or industry value chain. These automated business processes often extend beyond the 'borders' of a company and are indirectly 'linked' to every online computer within the world. Due to the ubiquitous nature of public and private IT networks and ultimately the Internet, this connectivity introduces additional threats to companies and to the financial information held in electronic form within companies.

In addition, a new paradigm of auditing needs to be accepted and implemented to match the relentless pace of technological change (Onions, 2003). Corporate-wide networks enable companies to integrate global manufacturing, inventory record keeping, financial management and informative forms of corporate reporting (Vasarhelyi, 2002). Furthermore, Vasarhelyi notes that the exponential growth of online retailing, securities trading and procurement systems, again emphasises the need for continuous auditing.

7.3.2 What is Continuous Auditing?

Today, one needs to provide continuous assurances about the quality and credibility of the information presented. Even with the advances in auditing tools and techniques, auditors still provide assurances months after the transactions occurred and run their tests in batch mode. With real-time information systems and decision makers wanting up to the minute information, there is an even greater need for continuous auditing and 'assurance on demand'. Continuous auditing is defined as (CICA/AICPA, 1999): *"a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter"*.

To comply with this definition, orderly processes are necessary to provide an effective audit trail for the flow of data. Such processes are critical if auditors are to adequately assess strengths and weaknesses in the information security and internal control environments, as well as perform analytical tests and audit transactions in real-time (Warren & Parker, 2003).

Traditionally, auditors test controls retrospectively and on a cyclical basis, often months after the transactions have occurred. In addition, their testing procedures have often included only a sample of business activities or transactions. Therefore, they can only provide a 'snap shot' view. Continuous auditing changes the audit paradigm from periodic reviews of a sample of transactions to ongoing audit testing of 100% of transactions. Essentially it is technology that

enables auditors to perform the testing of control and risk assessments in real-time.

The 'power' of continuous auditing therefore lies in the intelligent and efficient testing and notification of gaps and weaknesses to allow immediate follow-up and remediation (GTAG3, 2005). The testing should cover two main areas:

- *Continuous Control Assessment* – which focuses as early as possible on control deficiencies.
- *Continuous Risk Assessment* – which highlights processes or systems that experience higher than expected levels of risk.

The key to understanding the two areas of assessment in relation to this research project is to understand that controls exist to help mitigate risk (as discussed in Chapter Four). The identification of *control* deficiencies highlights areas of potential risk. Conversely, by examining *risk,* auditors can identify areas where controls are inadequate, hence, the focus of continuous auditing ranges from controls-based to risk-based. The analysis techniques range from real-time review of transactions (testing detailed information down to source level) to the analysis of trends and comparisons over time.

Continuous auditing therefore systematically and continually tests transactions using intelligent software tools. The auditor prescribes the criterion and the process identifies anomalies/exceptions for which additional audit procedures should then be performed. Depending on the findings, the auditor may issue a report. The growth of ERP systems, increased bandwidth and use of the Internet, the speed of processing and the globalisation of business, have all contributed to the development of more intelligent software tools (Rezaee et al., 2002; Vasarhelyi, Alles, Kogan, 2003). These developments provide management and auditors with the ability to better capture and analyse key data for decisions. The use of intelligent agents, embedded in audit modules to monitor and trigger

alarms when unusual transactions or patterns occur, provides management with tools to better monitor business processes (Warren & Parker, 2003).

Warren and Parker (2003) claim that these software tools are especially suited for companies with high volume and high-speed applications and which have complex information technology environments (e.g. banks and financial services companies). They feel that in these environments it is necessary to have in place a process, such as continuous auditing, that will not impede the flow of data. Furthermore, the Internet has created an electronic means for providing information to interested parties, such as investors, regulators and customers on a global real-time basis. It is therefore logical that management will be required to put in place internal controls that protect the integrity of information from unauthorised access or use, and that such measures will become part of the company's overall monitoring platform.

To reiterate, according to The Centre for Continuous Auditing (Texas A&M University, 2005), the future audit processes will likely encompass auditors using interrogative software in performing their audit procedures as well as embedding audit modules into the company's IT environment. They propose this will be necessary because *"transactions lose their identity during processing"* and auditing these transactions to determine their validity will require real-time audit processes. This will assist in providing assurances on demand.

As emphasised by Vasarhelyi (2002), widespread availability of computer networking makes it possible to dramatically redesign the auditing architecture around online auditing. He proposes that if auditors perform reconciliations in an audit that these procedures can be *"wired-into"* software and performed daily. If out of balance conditions arise, alarms can be created. He further notes that this new audit approach will take the modern view of the company where a larger community of stakeholders actually have some economic interest in the company. The traditional or current auditing model is justified by the need for third party assurance on the moral hazard gap between owners and managers

(principals and agents). But as so succinctly posited, the current ex-post assurance methods are becoming progressively less reassuring (Vasarhelyi, 2002).

7.4 CONTINUOUS AUDITING TECHNOLOGIES

It is stressed that technology can provide a new toolset to measure performance and provide assurance, which may reverse the progressive decrease in relevance of accounting measures and their attestation (Vasarhelyi, 2002). Now auditors can implement an independent superstructure of measurements linking related processes and thus rely on the measures through a toolset of automated links among independent entities. For example, intelligent software agents can replace confirmation of receivables or payables. Agents could render continuous queries into third party systems, obtain confirmation of balances and transactions, and reconcile cut-off and float differences. These measurements are more sensitive to fluctuations and show discrepancies with greater sensitivity.

The concept of continuous auditing technologies is that they can run continuously in the 'background', within the company's information systems, in a similar manner to virus-scanning programs (Hunton et al., 2004). Onions (2003) claims that the concept *"electronization"*, has a natural outcome for the audit process to become 'electronized' by using technology. As noted, these technologies need to meet the auditing requirements in order to verify that a real-time accounting system produces accurate and reliable financial information, and the testing of controls must be done simultaneously with substantive tests of transactions (Helms & Mancino, 1999; Rezaee, Elam, & Sharbatoghlie, 2001).

This section will introduce a few technologies that can be used within a CA environment; however, technologies currently used by auditors such as CAATTS, automating traditional auditing methods and testing historic information in batch mode, will not be discussed.

7.4.1 Embedded Audit Modules (EAMs)

Embedded Audit Modules are audit related routines within the source code of a software application. They are designed to continuously monitor events which are significant to the audit and then report on them. They do this by identifying and flagging transactions which meet pre-set criteria. These transactions are then reviewed by the auditor. This can be done in real-time or in batch mode (Braun & Davis, 2003).

It is important to note that EAMs are highly automated and function with little intervention. They are used by auditors in two main ways. Firstly, when testing transactions, EAMs can be used to identify large numbers of transactions for substantive testing. Secondly, EAMs are also useful in the evaluation of control risk (Cerullo & Cerullo, 2004). They test controls by checking if transactions are processed according to policies and procedures.

Negative aspects of EAMs include the fact that they are built into the application. Not only does this mean that a substantial amount of planning is required in designing an application, but also that programming expertise is required to implement and maintain the module. Changes to the application could also require the EAM code to be reviewed. Auditors would need to have a close relationship with the client's system administrators (Braun & Davis, 2003).

EAMs are generally based on artificial intelligence or intrusion detection as they are embedded within applications and trigger anomalies. This leads to the next section on artificial intelligence (AI).

7.4.2 Artificial Intelligence (AI)

Various types of AI software can be used in continuous auditing, including Intelligent Agents, Expert Systems and Neural Networks. The objective of AI should be *"to provide better information and rules for better results"* (Warren & Parker, 2003).

7.4.2.1 Intelligent Agents

Intelligent Agents are audit programs which use a set of auditor-defined heuristics to analyse a transaction set. This proactive software looks for patterns of activity or suspect and unusual activities or trends. If no explanation is found for the unusual activities detected, it then alerts the auditor to the presence of the unusual activity (Kogan, Sudit, & Vasahelyi, 2000).

These intelligent agents are sometimes referred to as digital, control or autonomous agents. A widely accepted definition proposed by Russell and Norvig (2003, p.32) states that *"An Agent is anything that can be viewed as perceiving its environment through sensors and acting upon that environment through actuators"*. Agents differ from general software in that they can be reactive or proactive (Kogan, Nelson, Srivastava, Vasahelyi, & Bovee, 1998).

According to Woodroof and Searcy (2001) in the context of continuous auditing, an agent is a set of electronic instructions (encapsulated in software) that acts on behalf of the auditor in a semi-autonomous manner to perform some service related to the subject matter being audited. These agents (sometimes referred to as *tools*) often make use of technologies such as digital analysis and data mining.

Many authors have suggested using agents for various purposes in auditing. These include gathering or sorting information, but also to perform analysis and make decisions related to financial data. FRAANK (Financial Reporting and Auditing Agent with Net Knowledge) is an example of such an agent. FRAANK is designed to extract data from *natural text* financial statements and translate them into XBRL (tagged) statements (Kogan et al., 1998). This could be used in numerous ways in a continuous auditing system. For example, when new statements are produced in XBRL, they need to be translated and then compared to historical statements, which may be in a legacy system format.

7.4.2.2 Expert Systems

Expert Systems are able to process huge amounts of data in an intelligent way, mimicking human analysis. Expert systems interpret data to find patterns where no previous patterns were known to exist, while the traditional audit procedures are limited to finding pre-determined patterns known to identify anomalies or exceptions (Dalal, 1999). Therefore, an expert system is a software application that contains subject specific knowledge and therefore is a knowledge based system. Knowledge engineers build expert systems to assist with problem solving.

To summarise, expert systems are constructed by obtaining knowledge from human experts and coding it into a form that a computer may apply to similar problems. This reliance on the knowledge of a human domain expert for the system's problem solving strategies is a major feature of these systems (AAIA, 2006). Therefore expert systems can be viewed as an extension of the auditor. The methods employed, using expert systems, have become more refined over the last decade and their reasoning techniques have become more sophisticated.

7.4.2.3 Neural Networks

One of the more recent AI related technologies to garner attention is Neural Networks. Neural Networks process data in a way similar to the human brain and are based on algorithms developed to learn the relationships within data (Warren & Parker, 2003).

Based on the researcher's personal experience, a neural network can be incorporated into a financial system (i.e. credit card) and used to help identify purchasing patterns. When irregular transactions occur, the neural network triggers alerts for possible fraud detection as it functions on a predictive modelling basis, thereby recognising irregular purchasing patterns.

Like expert systems, neural networks can analyse huge sets of data (in fact because they learn by trial and error, larger data sets improve the accuracy of the

neural network over time). They work by recognising new patterns within the data. Neural networks can be used in many areas, including both risk assessment and assessing internal controls. They can also be applied as a forensic accounting tool to proactively predict the occurrence of fraud (Cerullo & Cerullo, 2006). AI and related technologies are becoming more commonplace in everyday life and will soon be essential tools in real-time accounting and auditing systems.

7.4.3 Data Warehouses and Data Mining

The tremendous growth in electronic storage capability and reduced storage costs accommodates the storing of huge amounts of data generated by corporate information systems. This capability has resulted in the need for the development of efficient methods to store and retrieve data. It is pointed out that *"data warehousing refers to the process of storing data in data warehouses according to predetermined criteria so that retrieval of data for various purposes can be accomplished in an efficient and effective manner"* (Abdolmohammadi & Sharbatouglie, 2005, p.57).

Abdolmohammadi and Sharbatouglie (2005) continue and add that a well designed data warehouse enables companies to use various data from online transaction processing systems which have become more common in recent years. Other sources of data, such as customer credit ratings obtained from credit agencies, can enrich the database so that more powerful data analysis through data mining techniques can be used to generate reports and assist decision-making.

It is proposed that data mining is an enabling method for continuous auditing in the sense that it finds patterns in data sets through statistical analysis (Abdolmohammadi & Sharbatouglie, 2005). It is also suggested that auditors use data mining software to perform analyses and tests of online transactions when conducting risk assessments (Bierstaker, Burnaby & Hass, 2004). David and Steinbart (2000) go further and suggest the data mining can be used for more

than statistical analysis and should include artificial intelligences to explore and analyse the vast amounts of data stored in data warehouses.

7.4.4 Business Intelligence

As pointed out by Warren & Parker (2003), Business Intelligence (BI) has 'grown' out of systems which were popular in the earlier 1990s, such as decision support systems (DSS) and executive information systems (EIS). BI can be defined as the use of corporate information databases and warehouses to assess KPIs and compare what has occurred against metrics and then perform analyses of the trends. BI is a powerful tool for the interrogation of databases.

Some researchers include *"business activity monitoring"* (BAM) as an element of BI and propose that *"BI can be seen as another way of continuous data gathering and monitoring"* (Warren & Parker, 2003, p.36). However, BAM goes one step further than BI and includes Internet and related technologies.

In summary, some of the attributes of business intelligence are comparable to several continuous auditing attributes. This can be noted by SAS (2006) which describes business intelligence as the power to make better decisions. SAS states that BI allows one to *"understand the past, monitor the present and predict outcomes"*.

7.4.5 Extensible Business Reporting Language (XBRL)

Even though technology has advanced and there are methods that compile financial reports on a near real-time basis, the auditing profession has not yet been able to provide assurances that the information within these reports is 100% accurate. XBRL is an extension language of XML and was created as a language that can possibly provide seamless, continuous financial reporting which can lead to 'accurate' real-time reporting of financial reports.

XBRL allows tagging of data so that it can be accepted directly into the recipient's database for further analysis (see www.xbrl.org). In addition, XBRL

has the capability to populate auditor databases for immediate evaluation by auditors and their automated tools and techniques. Following this, statistical methods such as data mining can be used to identify high-risk transactions (Rechtman, 2004). XBRL is designed to make it easier to prepare, publish, exchange, acquire and analyse accounting and business related information (Flowerday & Von Solms, 2005b). Alles et al. (2005) argue that Section 409 of the Sarbanes-Oxley Act will eventually require assertion and assurances of continuous monitoring of corporate controls and meta-controls at each process (process assurance). These will be used to improve the quality of the data being transmitted from process to process.

Process assurance leads to the auditing of transactions that should be carried out in real-time as business is conducted in real-time (Onions, 2003). Onions, from the European Centre for Continuous Auditing, proposes Extensible Continuous Auditing Language (XCAL) which, like XBRL, is also an extension of XML. XCAL, together with expert systems, will verify transactions at keystroke entry level and perform a more thorough interrogation of the data in a data mine before assurances are given.

It is proposed that if the data in the sub-ledgers is fraudulently or erroneously entered, it will carry through to the general ledger. It is this data that will be used by XBRL from the general ledger in formulating the financial reports (Onions, 2003). This line of reasoning is that the auditor could not report on or give opinions and assurances that the integrity of the data in the general ledger is correct. They would first have to follow a process of 'testing/checking' the entries and transactions in the sub-ledgers.

Onions (2003) emphasises that one should follow the data path from data entry all the way through to the posting in the general ledger. This is a mammoth task to conduct manually, or with CAATTS, and that is why the traditional audit takes a sample of transactions for testing. Even using CAATTS, the testing is done in

batch mode and so generally only a sample is tested. Or else if tested in its entirety, it is done after the fact and the reports are historic, due to the time lag.

The advantage of continuous auditing is that with the advances in technology, i.e. more powerful processors and increased bandwidth, every transaction can be checked. To increase the quality of the audit, every transaction should be stored in a data mine. The aggregated data is trawled by expert systems searching for patterns, heuristically with rules specified by the auditor (Onions, 2003). This dual pronged approach of testing or checking transactions in a data mine and at keystroke entry is continuous in nature and should provide near real-time assurances that the information in the ledgers has not been compromised.

7.5 CONTINUOUS ASSURANCE

Dull and Tegarden (2004) recommend that in order to provide continuous assurance the auditor should use control charts and methods that examine and report on the state of control of the underlying systems and that trend analysis be done for the analytical review. Moreover, they emphasise that the use of technology should be employed to actually audit, as opposed to using technology to automate manual auditing procedures. Plus GTAG3 (2005, p.10) adds that by *"assessing the combined results of the continuous monitoring and auditing processes, auditors are able to provide continuous assurance"*. This is illustrated in Figure 7.2. This procedure should ensure that the information produced for decision-makers is both accurate and reliable.

To draw attention to this issue in December 2002, the American Institute of Certified Public Accountants (AICPA) established the Enhanced Business Reporting Model Committee to migrate the current reporting model to an online, real-time business-reporting framework. This framework calls for continuous assurance of the information being reported (AICPA, 2002). Modern-day business complexity and technology are attributes of companies that suggest

auditors will be required to develop new methodologies and processes for continuous assurance.

It is important to note that although continuous monitoring and continuous auditing may be similar in nature, particularly on the operational side, they differ in purpose and intent. This relates back to the agency – principal theory discussed in Chapter Two. *Management monitor and auditors audit*. The 'truth or true picture' of what management (the agents) is doing is provided by the auditor.

Vasarhelyi's (2002) remarks summarise this section that there is no continuous assurance without intense continuous monitoring, measuring and reporting. He states *"continuous assurance is the congruent electronization of a set of accounting, controlling, monitoring and auditing processes"*.

7.6 CONCLUSION

The OECD (2004, p.25) states that: *"In order to fulfil their responsibilities, board members should have access to accurate, relevant and timely information"*. However, how confident are the directors in their decision-making when the assurances as to the integrity of the information, are not provided until several months after their decisions have been made?

Therefore, management and auditors should focus on improving the internal controls and risk assessments, and thereby the integrity of information within financial reports. One cannot then but help improve corporate governance and investor confidence by providing real-time assurances. The day of the company's directors claiming *"I did not know",* in connection with errors and fraud within their company's financial statements and getting away with it, should be over.

Although there may be many *drivers* (e.g. compliance, risk management) or motivators behind the continuous monitoring and continuous auditing euphoria, the main enabler is technology. One should thus embrace technologies such as Extensible Business Reporting Language, Embedded Audit Modules, Data Warehousing, Data Mining, Business Intelligence, and Artificial Intelligence as one tries to meet the needs of the various company stakeholders, including the directors.

To emphasise an important point: the identification of control deficiencies highlights areas of potential risk. Conversely, the examination of risk through analytical procedures, such as trend analysis, by auditors can help identify areas where controls are inadequate. This leads to Chapter Eight that introduces and compares three proposed continuous auditing models. This is done in order to illustrate *how* these technologies and the continuous auditing process is intended to function.

Chapter 8

CONTINUOUS AUDITING METHODS AND MODELS

"There's nothing remarkable about it. All one has to do is hit the right keys at the right time and the instrument plays itself."
- Johann Sebastian Bach, (composer, 1685-1750)

8.1 INTRODUCTION

Chapter Seven addresses *what* continuous auditing (CA) entails and this chapter addresses *how* continuous auditing can be performed. There are different approaches and methods for performing continuous auditing. This is due to the level of automation, which is influenced by the system's design and implementation. These continuous auditing processes generally use the technologies discussed in Chapter Seven to constantly monitor and report on significant audit events. These events or exceptions are found either within the system itself or the data used by the system. Nevertheless, as pointed out by Rezaee et al. (2002), some auditor intervention may still be required to query unusual patterns and isolated exceptions.

Probably the first continuous auditing process or model proposed was in a 1989 paper titled; *Continuous Auditing of Database Applications: An Embedded Audit Module Approach* by Groomer and Murthy. Following this, one of the early models implemented was the *Continuous Process Auditing System* (CPAS), which was developed at AT&T Bell Laboratories. This was a methodology for internal auditing of large *"paperless"* real-time systems (Vasarhelyi & Halper,

1991). This CPAS model appears to have formed a basis for many of the later models, including the ones to be discussed in this chapter.

Three of the better-known continuous auditing models will be discussed and explored in relation to their *focus*, *implementation steps* and their major *component parts*. The first model to be addressed is *A Continuous Auditing Approach* developed by Rezaee et al. in 2002. Then *A Model for Secure Continuous Auditing* by Onions (2003) is summarised. Finally, the *Continuous Audit: Model Development and Implementation within a Debt Covenant Compliance Domain* by Woodroof and Searcy (2001) is examined. Following the summaries of these models, an evaluation of their methods against a common criterion is conducted to assist in appraising them. Finally, at the conclusion of this chapter practical suggestions for the future of continuous auditing are proposed.

8.2 THREE CONTINUOUS AUDITING MODELS

A synopsis of three better-known continuous auditing models is presented within this section.

8.2.1 A Continuous Auditing Approach (Rezaee et al. 2002)

A conceptual framework, described as *A Continuous Auditing Approach*, is laid out within a paper that explores continuous auditing methodologies. Rezaee et al. argue that one of the most complex and challenging aspects of building a continuous auditing capability is the standardisation of data. Diverse file types and various record formats produced by various sources, including legacy systems, must be accommodated. This creates a risk of duplicating records and introducing errors that could negatively affect the integrity of information.

Rezaee et al. (2002) propose two approaches that are described for the collection and storage of data. The use of a *"scalable audit data warehouse"* is the first approach. A repository for storing transaction data produced by different business systems, a data warehouse, is designed. This data warehouse should be

scalable, allowing for increasing amounts of data as audits progress. This approach is recommended for dispersed systems with varied data formats. It can be expensive, particularly when embedded audit modules are required within complex legacy systems. In such cases, the second approach may be more beneficial. Instead of building a data warehouse, subject specific audit data marts are used to automate the capturing of relevant data, and the auditing and reporting processes.

This continuous auditing model is capable of running on a distributed client/server network and is also web-enabled for transmitting data to audit workstations. The model is executed and explained in the four points listed below and is illustrated in Figure 8.1.

1. The data is collected from transactional systems. This is done by linking to tables, via FTP (File Transfer Protocol), storage drives or via modems. The data is then stored on an audit server.

2. Once on the audit server, data is extracted from a variety of platforms and systems. Data standardisation is therefore required. Standards and formats are developed for storing data in the data warehouse/mart. The data is then transformed by cleaning, validating, restructuring and 'scrubbing' it with business rules.

3. An enterprise-wide data warehouse is not always needed, as it may be too expensive and complex. Instead, the required data could automatically be fed into several data marts. The data marts contain metadata, which details the source transactions and the ETL (Extract Transform Load) process as well as the tests that take place. The metadata may, for example, include detailed file definitions, business rules and transaction process flows.

4. Standardised tests are created to run within the data warehouse/mart. The tests are created either to run continuously or at predetermined intervals (end of a business period e.g. daily, weekly or monthly). The tests are designed to automatically gather evidence and issue exception reports.

As noted, the model illustrated in Figure 8.1 does not require a company-wide data warehouse. In this solution, many subject specific data marts are automatically fed data and periodically selected data is extracted. This data is selected according to an audit-testing plan; this reduces the number of elements needing data transformation and mapping.

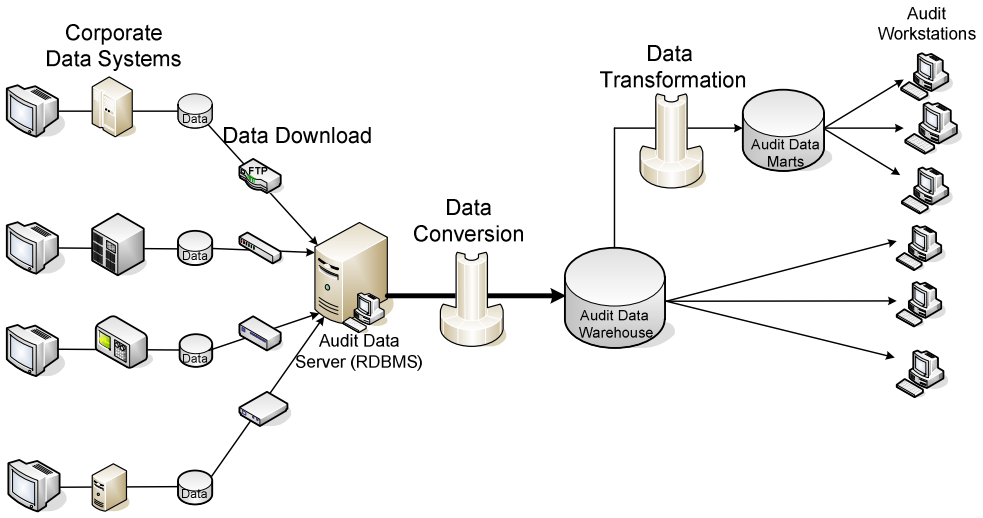

Figure 8.1: Continuous Auditing Approach (Rezaee et al., 2002)

The model consists of the following components:

- **Corporate Data Systems:** Includes ERP solutions such as SAP, BaaN, PeopleSoft, Oracle or SQL. The data may be in various formats such as VSAM, IMS, ASCII, MDB, CSV, XLS or TXT.

- **Audit Data Server**: To aid easier access, analysis and reporting, the data collected for various business units' data marts is physically stored in the audit data server.

- **Audit Data Warehouse**: Once converted, selected transactions, which are deemed to pose an audit risk, are collected and stored in the audit data warehouse.

- **Audit Data Marts**: Standard metadata containing the complete details of source transactions and the Extract Transform Load process (e.g. file definitions, business rules, transaction process flows) is stored in the relevant data mart. A data mart may be for a particular business unit or several highly interrelated business units.

- **Audit Workstations**: As illustrated in Figure 8.1, the 'end users' interact with the data mart or data warehouse via audit workstations. Users include auditors, business\unit managers and corporate security officers. There are two generic categories of end-users described: Oversight users only need to access exception reports; analytical users formulate their own queries and need to interact with the data. The latter requires advanced data extraction and analysis software on the audit workstation to assist with data conversion and transformation.

This model has the widest scope of the three models and appears to focus on the standardisation of data. It depicts a relatively generic solution to continuous auditing. The next model focuses more on information integrity and secure continuous auditing.

8.2.2 A Model for Secure Continuous Auditing (Onions, 2003)

The aim of this model is to introduce the concept of CA as a new paradigm. It suggests that in order to guarantee the integrity of accounting information captured in ledgers, it is necessary to monitor all keystrokes and transactions

within the system. It is then necessary to search for patterns, trends and exceptions in groups of transactions. Expert systems are used as the means by which to search transactions for patterns. These actions concern the three basic areas of data examination within a continuous auditing system. These are: *keystroke level*, *transaction level* and *transaction pattern level* data examination (Srinivas, 2006). All three areas of data examination are required to make the continuous auditing system both effective and comprehensive.

- The first of these areas, *keystroke level* data examination, involves monitoring database utilities and applications for commands which could cause fraud or error. Database utilities allow users to modify and update a master file, bypassing the normal safeguards present in the accounting systems itself. Committing this type of fraud normally entails using a Database Management System (DBMS) and Structured Query Language (SQL) commands or other database interfaces such as the Data File Utility (DFU) on the IBM AS/400. The fraudster would need to log on using a supervisor/administrator password, which is possible if security of these database utilities is compromised. In many companies, administrator passwords are known to many people, or are not regularly changed or at times never changed from the defaults created during installation. The disadvantage of keystroke monitoring is that it needs to be embedded in the operating system of the computer and, as with a virus checker, uses processing power and therefore adds to the 'load' on the machines.

- *Transaction level* data examination involves auditing and reporting on each transaction as an isolated entity. This is done *ephemerally* (briefly) - the transactions are tested at the time of entry. It is then ascertained whether each transaction meets the pre-specified rules for transactions. These may be business rules or even rules dictating what actions are permissible for certain users. This is done in conjunction with performing certain analytical functions. These operations would need to

be performed on the transactions in real-time rather than batch. Most of the current CAATTs run in batch and would have to be modified.

- After a transaction has been examined, it may be added to a data mine for possible further examination. *Transaction pattern level* examination involves examining the effects of transactions, as a whole, over a longer time period (perhaps even years). Expert systems and rules based criteria are used to identify patterns in the groups of transactions, which could together result in fraud or error. The rules would be similar to virus definitions and would be made available for different industry types.

A problem experienced when attempting to use Expert Systems is that each available software package has a different data schema. It would be very costly and time-consuming to create expert systems for each application. The suggested solution is to create a generic master file and transaction layout, which could be used regardless of the application data schema. This newly defined generic schema for a transaction would allow one Expert System to trawl through the data mine. This schema would be defined using eXtensible Continuous Auditing Language (XCAL). As previously noted (in Chapter Seven) XCAL, like XBRL, is XML-based. One advantage of XCAL is affordability; therefore it is not just large companies that can implement its use.

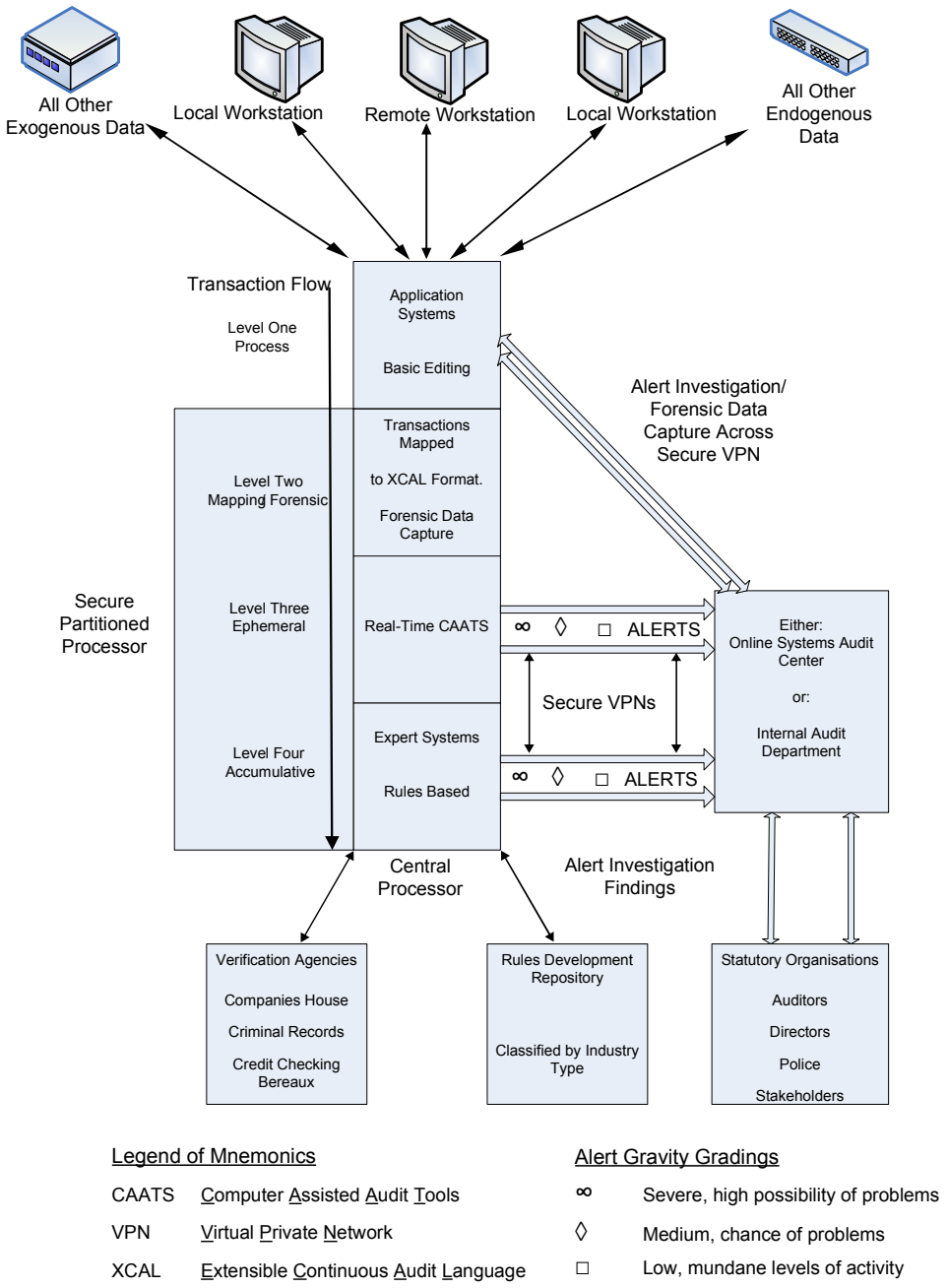

Figure 8.2: A Proposed Model for Secure Continuous Auditing
(Onions, 2003)

As shown in Figure 8.2 above, the model consists of four 'levels', which describe the steps involved. These levels describe the steps taken when the model is

running and are not the same as the data levels mentioned previously in this section. The previously mentioned levels are the three areas of examination for the model to be comprehensive and effective.

The four implementation steps for this model are:

1. Transactions and data from various sources are entered for processing. Basic editing takes place within the application. The applications appear to run as normal, without delay.

   The three remaining steps are partitioned and secured from all users (including Administrators). These are installed and maintained by proposed government approved Systems Audit Centres.

2. Transactions and keystrokes are mapped to XCAL schemas. This is done in real-time. Transactions are captured forensically on a daily basis so that they may be submitted as evidence, should fraud or error be detected. DBMS utilities are used to capture the data to a secured storage medium. In the UK, data needs to be exactly as the user entered it in order to be admissible as evidence within a court of law, thus the data may not be encrypted when captured forensically.

3. Real-time CAATT processing is used to check transactions and keystrokes. This runs slightly after the application (first) steps, but only by nanoseconds. Rules for this stage of auditing will vary according to transaction type. They are compiled from knowledge gathered from experienced auditors and forensic accountants.

   Alerts may be sent to a proposed Online Systems Audit Centre (OLSAC) via secures VPN's (Virtual Private Networks). OLSAC is intended to be a group of professionals, skilled in information systems, business processes and auditing, which monitors alerts and investigates them

online. OLSAC will be authorised to do this by the government or the professional accounting and auditing bodies. OLSAC methodologies and techniques would differ from current audit methodologies. For example, the current auditors would still prepare the annual financial audit report, to which an OLSAC certificate is appended. This certificate confirms that the systems were operated and investigated according to current standards. It would also detail the alerts of the past year and the actions taken as a result of these alerts.

The alerts, which are sent out at Step Three, are graded according to gravity (low, medium, severe). Transactions are stored at this step for a day, after which they pass to Step Four where they are stored for years.

4. Expert Systems look for patterns in the data which are pre-defined by expert rules. These rules are formulated from knowledge elicited from standards, laws, best practices, historic transaction patterns and the expert's experience.

   Artificial intelligence within the expert system will also allow new heuristic rule sets to develop. These are automatically included into the ongoing analysis of the expert system. All the rules are aggregated together in a single separate knowledge entity known as the *rules repository*. Here, the expert system stores as much information as possible about a given subject, in this case business rules, which are used in conjunction with heuristics to analyse the transactions. Newly formulated rules are delivered and installed via the Internet with release level techniques, much like an antivirus update. Rules will be classified by industry type, as industries may have subtle differences, although the financial ledger systems should be similar.

The expert system is continually analysing the data and asks thousands of *"if then"* questions. These questions relate to both single transactions and groups of transactions.

The alert processing system of Step Four is similar to that of Step Three. Alerts are also graded, but Step Four alerts are more likely to be complex in nature. The alerts are sent to auditors over secure networks such as VPNs.

In Step Four, the system would also have the ability to communicate with various agencies in order to verify data from transactions. These verification agencies may include criminal record databases and various credit bureaus. An example where fraud could be detected in this way is where new supplier details are checked against Companies House. Postcodes or directors' names corresponding to those of employees may reveal fraud. This ability to communicate with external agencies is facilitated by *Web Services*. Web services use XML to exchange data and parameters between software applications via a network such as the Internet or a VPN.

This model focuses primarily on data integrity. It also attempts to find a solution to the problem created by trying to use expert systems where a variety of data formats are present. In the next section the last of three models is discussed.

8.2.3 Continuous Audit: Model Development and Implementation within a Debt Covenant Compliance Domain (Woodroof & Searcy, 2001)

This model is limited; it is discussed in relation to debt covenant compliance. The model makes use of web-enabled technologies and draws attention to the need for a reliable and secure system. The need for the production of *'evergreen reports'* is also introduced. Evergreen reports are reports generated on demand and usually viewed through a web site. The model is based on a database of

transactions (journals and ledgers) on the client's system, with a web interface for the auditor to use.

A debt covenant is the legal agreement between a lender and a borrower. It specifies the terms of the loan (the term, interest rate and payment information) as well as required collateral and what values of key variables constitute compliance (and how to remedy non-compliance). The model allows compliance with the debt covenant domain to be monitored via the web by the lender. Loan Officers are presented with a web page listing all loans for which they are responsible, as well as the debt covenant agreement and the relevant criteria related to the loan. This allows the loan officer to continuously monitor whether the actual values of the client's variables are in compliance with those in the covenant agreement.

The five implementation steps involved in this model are:

1. The loan officer requests an evergreen report by sending the client's loan covenant parameters to the auditor.

2. Agents and sensors within the client's system monitor the transaction data for exceptions to pre-specified rules. These exceptions may trigger alarms, and alerts, which are then sent to the auditor. The rules check the reliability of the system (Woodroof and Searcy suggest using continuous SYSTRUST), the fairness of the representation of financial reports and compliance to third party contracts (i.e. debt covenant agreements).

3. An *intelligent agent* on the auditor's system requests an agent on the client's system to retrieve the client's real-time balances of accounts via stored procedures in the client database. The client's intelligent agent then creates a *backend* page from the information retrieved by a stored procedure. These pages are never called for directly and do not have a user interface; they exist only to facilitate the use of intelligent agents.

4. If more information is returned than is needed in the backend pages, the intelligent agent extracts the information relevant to the *contract* (in this case debt covenant compliance). This is done in a temporary workspace, which is parsed by the intelligent agent for values relevant to the debt covenant compliance. The information is checked for compliance, i.e. the actual event or process is checked against an acceptable standard for that event or process. If exceptions or anomalies occur, these are flagged and the auditor is notified so that action may be taken.

5. An evergreen report is generated and displayed to the loan officer. This details three levels of assurance. Level One is an assurance of reliability. If there is Level One exception, no further analysis is performed. Level Two offers an opinion on the fairness of real-time financial statements. Level Three provides an analysis of technical violations of third party contracts (in this case debt covenant compliance is assessed).

Due to the reports being pulled (produced on demand) as opposed to being pushed to the user as in the previous two models, this model is less suited to using XBRL-based reporting.

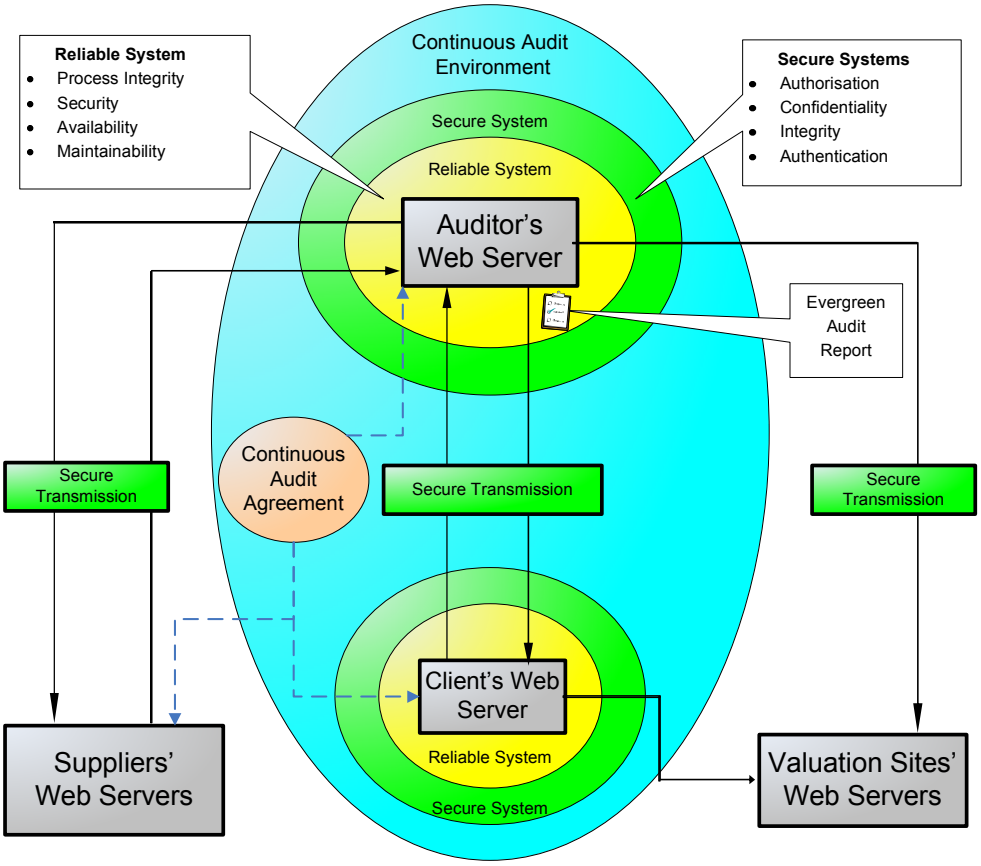

Figure 8.3: The Model of a Continuous Audit (Woodroof & Searcy, 2001)

The component parts of this continuous auditing model as depicted in Figure 8:3 include:

- Various interconnected web servers:

  The participating web servers are interconnected and are given authority to communicate. The auditor has controlled access to the client's database through the *client's web server*. In turn, approved third parties and external users have limited and controlled access to the client's database through the *auditor's web server*. Third parties are suppliers and customers who have agreed to a continuous auditing relationship with the client through the auditor. These third parties may represent customers, vendors (suppliers of merchandise) and financial institutions

(suppliers of capital). Automatic electronic confirmation of account balances such as accounts payable, cash and accounts receivable would be possible. The *valuation site's web server* represents websites containing information on adjustments made to various accounts, for example, the market prices for shares held for resale.

- Continuous audit environment:
  This is described as the data flowing through the client's system that is continuously monitored and analysed using devices integrated within the system. Auditors are notified via the Internet of exceptions to predefined rules by means of triggered alarms. The alarms notify the auditor of potential deterioration or anomalies in the client's system. The aim is to collect information (for example market values and estimates) in real-time so that real-time assurances can be provided by reflecting real-time information in the reports produced.

  Three levels of assurance are provided, each having a different degree of significance and requiring the auditor to take different actions.
  - Level One is assurance regarding the reliability of the client's system and the security of the data transmitted.
  - Level Two is an opinion on the fairness of the real-time financial statements produced by continuous assurance.
  - Level Three concerns the client's compliance to a domain specific agreement with a third party, as detailed in the continuous audit agreement.

- Characteristics of a reliable system:
  Continuous assurance is considered worthless if the underlying reliability of the systems producing the assurance is in doubt (as noted in Chapter Six). Therefore, an adaptation of SYSTRUST from a periodic assurance to a continuous assurance is suggested.

- Characteristics of a secure system:
  All transmission of information between parties should be authorised, be confidential, have integrity, and be authenticated. There may be other reliability and security concerns which fall outside the continuous auditing environment yet impact on it. These include the reliability and security of web valuation sites referenced in the audit and reliability and security of the ISPs (Internet Service Providers). These concerns may be addressed by services such as Veri-Sign, Better Business Bureau, TRUST-e, International Computer Security Associations and WebTrust.

These components together form the basis of this model. This third model differs from the first two in that it functions in a limited business domain (debt covenant compliance) and is web-centric.

8.3 COMPARISON OF THE THREE CONTINUOUS AUDITING MODELS

This chapter has discussed three well-known continuous auditing models each with their own specific approach. It appears that the most generic model by Rezaee et al. (2002) aims to discuss firstly a continuous auditing methodology and secondly, to address the problem of data standardisation, whereas Onions (2003) focuses more on preserving the integrity of data and overcoming the problem of data formats, for which XCAL is suggested. The focus of Woodroof and Searcy's (2001) model dealt more with developing a working prototype of a continuous auditing system, and the scope of the model was limited to a single business domain – debt covenant compliance. Also discussed was the mechanics of each of the models explained in terms of the steps involved. In addition, several of the component parts of each model were listed as they were to be found in the source literature.

To further assess these models, comparisons will be drawn and commonalities between the technologies within the models will be discussed. To perform the

assessment of these models, consideration should be given to how accuracy and reliability of financial information is validated. As noted previously in the context of this research project, *Accuracy* refers to how fraud and error in transactions are detected and how possible material misstatements in financial records are detected. *Reliability* is concerned with the confidentiality, integrity and availability of the system; specifically the internal controls are examined.

Thus, the three models are examined with regards to how they validate *Accuracy* and *Reliability* of transactions. Other important aspects of the continuous auditing models are also compared and these include: the real-time nature of each model, the reporting method used and how the problem of differing data formats is addressed. This comparison was also published in an article by Flowerday, Blundell and Von Solms (2006), which is presented in a tabulated form below.

Table 8.1: Comparison of Three Continuous Auditing Models
(Flowerday et al., 2006)

	Rezaee et al. (2002)	**Onions (2003)**	**Woodroof & Searcy (2001)**
Accuracy **(Fraud and Error) within Transactions**	Standardised audit tests are built into audit data marts. They run either continuously or at predetermined times. These gather evidence and then generate the relevant reports.	Transactions are checked both at time of entry and later. CAATTS (Real-time, not batch) Expert Systems (not in "real-time" but running continually)	Rule-based detection by intelligent agents. Data is analysed by devices integrated into the system.
Reliability **of Internal Control System**	CAATTS are used. These include Integrated Test Facilities (ITFs) and Parallel Simulation. ITFs are used to verify correctness and completeness of processing. Parallel Simulation tests assess effectiveness of control activities.	Parsing of keystrokes to detect database management utilities. Password control. Operating System's security. Audit logs. Web services verify information (e.g. new supplier's credit history checked).	Adapt and apply SYSTRUST principles. Web-based valuation sites. Must be in the auditor-defined rules for the Intelligent Agents.

Real-Time	Real-time processing is the aim for this system.	All proposed systems run in parallel with operational systems in real-time.	Real-time reporting is one of the aims of this model. To this end, information must be collected and monitored in real-time.
Reporting Method	Web enabled data delivery of data to auditors' workstations, where reports can be generated (possibly by GAS).	Graded alerts sent through Virtual Private Networks (VPNs) to audit department/OLSAC. The alerts are graded by gravity (three levels).	Three levels of reporting, alerts are sent to the auditor via email. Level 1: reliability of the system or security of the transmission. Level 2: transactions and processes. Level 3: technical violation of 3rd party agreement. 3rd party and auditor notified by email. Evergreen reports are produced on demand through a web interface - Information *pull* approach. (As opposed to XBRL reporting, this uses a push reporting method).
Proposed Data Format	Data Mart Data Warehouse XBRL	XCAL Data Marts	Does not interface with legacy systems

This table identifies a common criterion to which these three continuous auditing models are compared. As can be noted, they all address the same challenge (continuous auditing); however, each has a different and individual approach. Drawing on these models, the next section makes suggestions for future CA models.

8.4 SUGGESTIONS FOR FUTURE CONTINUOUS AUDITING MODELS

As previously stated, to meet the requirements of continuous auditing, any comprehensive CA model would need to have a dual-pronged approach, where both the system (internal controls) and data are simultaneously tested. This section draws considerably on all three models discussed in Section 8.2 and from

Flowerday, et al.s (2006) paper. Any future CA model would need to address the three sub-sections discussed in this section.

8.4.1 The Data Acquisition and the Data Format Problem

Before any auditing can take place, the data needs to be Extracted, Transformed and Loaded (the ETL process). Transactions from a variety of sources need to be extracted. Not all records or fields may be required; however intelligent agents and stored database procedures could be used to obtain only the necessary data (Rezaee et al., 2002). Once the data has been extracted from the various databases, this data can be used within CAATTs and off-the-shelf database applications (e.g. Microsoft Access), spreadsheets (e.g. Excel) or data analysis applications (ACL, IDEA, Monarch) (Champlain, 2003).

The creation of data marts and data warehouses is desirable and a capable Database Management System (DBMS) is required. Data standardisation necessitates the development of a series of standards for storing data in the audit data warehouse (Rezaee et al., 2002). Thus, in a continuous auditing system the data is extracted to data marts where standardised audit tests can automatically gather evidence and generate exception reports. The data mart also holds metadata documenting source transactions and the ETL process.

Next, there is a need to collect evidence on the quality and integrity of an electronic system that produces reliable and accurate financial data and information. According to Wessmiller (2002), technology must aid in verifying the integrity of data, because the conclusions in the auditor's reports must be based on accurate and reliable data in order to be deemed *trustworthy*.

8.4.2 Validating Transaction Accuracy

Once data has been collected and transformed, the transactions need to be assessed for the existence of fraud and error. Transactions are individually assessed, verifying their integrity and validating if business rules were followed.

Possibly the most common way of validating accuracy is by using CAATTS. CAATTS can be made to run as close to real-time as possible, and function while the data is flowing through the application system (Onions, 2003). Both analytical procedures and substantive testing should be applied to search for fraud and error. For example, common IT-based fraud schemes often involve the billing system, payroll system and cheque tampering. Further examples include ghost vendors, ghost employees and exploiting voids and returns (Taylor, 2005). These schemes often need to be identified at the transaction data level.

Once the transaction data has been examined by CAATTS and is captured within the database management system, alerts can be produced. For example, intelligent agents may be used to alert auditors if transaction values change too much from 'traditional' trends. The relevant transaction data then needs to be collected for future forensic analysis - possibly by moving the data to a secured partition or dedicated audit server. This may be achieved using FTP (File Transfer Protocol) and tape or other large-capacity storage devices.

Intelligent agents can then examine transactions and select those that should be set aside for further analysis. CIS (Continuous and Intermittent Simulation) can also be used for deciding which transactions require more detailed examination. Once the data has been standardised and stored, it may then be checked for groups of transactions and the cumulative effects of a series of transactions. Expert Systems and intelligent agents may be very useful for this purpose. Analytical procedures can also be used to create 'norms' which can be used as benchmarks.

8.4.3 Validating Transaction Reliability

Additionally there is a need to ensure security of the system. A system that is not secure is not reliable. As discussed in Chapter Four, ensuring security would involve examining internal controls. If the system is not reliable, the results from that system may not be viewed as trustworthy. Woodroof and Searcy (2001) suggest SYSTRUST (or a CA derivative of SYSTRUST), but as noted

previously, COBIT in conjunction with ISO 17799 could also be used. COBIT would address internal control related issues and ISO 17799 would aid in addressing information security issues.

When enforcing reliability through a system of Internal Controls, the aim is to provide confidentiality, integrity and availability for the data and information within the system. CAATTS, such as Parallel Simulation and Integrated Test Facilities (ITFs) can be used to achieve this. In this model, Rezaee et al. (2002) deliberated on Concurrent Audit Techniques for testing the effectiveness of a client's internal controls. Concurrent Audit Techniques include SCARF (Systems Control and Review Facility) and the snapshot approach. SCARF functions as an exception reporting system. It captures transactions meeting certain criteria (defined by the auditor) by using Embedded Audit Modules. The captured transactions are set aside for later review by an auditor. Embedded Audit Modules and the SCARF approach could be used to create alerts regarding the status of internal control systems, by checking if adequate controls are implemented (Rezaee et al., 2002).

8.5 CONCLUSION

This chapter is a practical chapter addressing *how* continuous auditing can be performed. Three of the more influential CA models were analysed and compared against the basic requirements of continuous auditing. As can be noted from their comparisons, each of the three models has their own unique way of addressing the CA challenge. There does not appear to be a uniform approach or a consensus on technologies used to meet this challenge. It is therefore necessary at this early stage of the development of continuous auditing to study varying approaches and build from these.

Suggestions are proposed for future CA models focusing on the core points to be addressed. These core points are the *standardisation of data* to enable effective analysis; the validation of the *accuracy* of the financial data and information; the

reliability of the system which processes and houses the financial data and information.

This chapter contributes to the overall research project in that real-time information systems, especially financial and accounting systems, which generate information used by decision makers, allows confidence when basing their decisions on this information. This information is more trustworthy in that assurances can be provided shortly after the information becomes available rather than months later, once periodic audits are performed.

This trustworthy information that has been continuously audited and assurances provided in near real-time terms, contributes to good governance (transparency, responsibility, accountability, fairness) and better decision-making. Therefore, investor and stakeholder confidence should increase and it will furthermore assist with compliance to various regularity bodies. In addition to validating the information's integrity, continuous auditing will assist the company in identifying fraud and errors far earlier than traditional methods and thereby allowing the company to act speedily on these findings.

Chapter 9

CAUSAL MODEL

"The solutions all are simple – after you have arrived at them. But they're simple only when you know already what they are."
- Robert M. Pirsig (author and philosopher, b. 1928)

9.1 INTRODUCTION

To propose a solution for any problem one needs to ensure that the problem itself is being addressed and not a symptom of the problem. At times, this in itself is problematical. For this research project, it was necessary to investigate several problem-solving methodologies in an attempt to correctly identify the problem and the most suitable approach to solving the problem. It was noted that methodologies such as 'soft' systems theory, were essentially developed for use in ill-structured problem areas. This is where uncertainty exists over what actions to take to overcome the problem (Flood & Jackson, 1991).

This is where systems thinking, i.e. *"the process of thinking using systems ideas"* (Checkland, 1999, p.5) was applied in a systematic way - choosing to address parts of the problem by investigating various topics which together represent a solution or the whole. The solution is presented in the form of a causal model, which has followed the cause and effect principles of traditional or hard systems theory. However, it has incorporated elements of soft systems theory where the principle of human behaviour, guided by conditions and boundaries (these could be referred to as rules), has been used.

A controlled and deterministic view of restoring trust is subscribed to rather than randomness that mutates into the solution, in order to solve the problem. In other words, a more structured approach to building and safeguarding trust is the goal of this study. First, this chapter discusses systems theory and problem solving, followed by causality. Finally, a solution is proposed in the form of a causal model and parts of the model are discussed.

9.2 SYSTEMS THEORY AND PROBLEM SOLVING

The concept of systems thinking first emerged within the field of biology and the study of organisms. This introduced the notion of 'the adaptive whole' where the entity can adapt and survive within the limits of a changing environment (Checkland, 1999; Hanson, 1995; Von Bertalanffy, 1968). Additionally, this whole is made up of 'more than the sum of its parts'.

The following example, where a university is used to illustrate this concept, is presented by Checkland. He points out that university degrees are awarded not by departments, but by the university as a single entity. Checkland (1999) explains that the authority to confer degrees is an *emergent property* of the entity as a whole. The emergent property of this research project would be *increased trust and control*. Checkland further explicates that the smaller 'wholes' (departments) have their own emergent properties; for example, the authority to deliver a particular course. Yet one should not overlook that the university is only part of a larger 'whole', the Department of Education, which has its own emergent properties and so on.

The concept of soft systems thinking follows the traditional hard views on systems theory; however, it focuses more on *human affairs*. Traditionally, systems thinking involved *natural systems* and *design systems*. Natural systems are biological. Design systems, such as Shannon's communication system (discussed in Section 6.2.3), is based within the engineering field and does not consider human activities.

It is argued that the key difference between soft and hard systems is predictability. The hard or traditional systems approach assumes that systems within the world can be engineered to achieve declared objectives. Contrasting this is soft systems, which due to the human element, proposes that the world is problematical and that the soft systems thinking provides a way of *conceptualising the world* and the action to undertake.

Elements of soft systems theory are relevant to this research project, as according to Checkland (1999), the hard systems approach is founded on identifying the right solution. If two researchers arrive at different conclusions, their observations must be faulty or incorrect in hard systems. Whereas the soft systems theory approach regards organisations as complex, ever-changing social entities whose nature is continually redefined by those within it. Therefore it is possible to get different answers.

A hard view of a problem regards it as real and solvable and assumes that the ends are easily and objectively definable (Flood & Jackson, 1991). An example to illustrate a hard system problem would be that of a road when it comes to a gorge. It might need to end or find a way over the gorge. The solution would be to build a bridge over the gorge so that the road can continue. However, in reality, many problem situations are not well structured and the end or solution can often not easily or clearly be defined. These problems can thus be seen as ill-structured or soft problem situations. In these soft problem situations, it is necessary to acknowledge the importance of people and human activity, thereby acknowledging that different viewpoints exist.

In summary, the soft systems methodology is not a solution oriented approach, but is useful in clarifying problems. Once a problem is clearly understood, other analytical techniques may be applied to define the solution, such as design systems theory. Flood and Jackson (1991) reiterate that soft systems methodology is a guideline for examining situations and there is no fixed set of

rules that govern its use. This is graphically illustrated in Figure 9.1 by Checkland and Scholes (1990, p.27). Their seven stages of soft systems methodology are divided into two larger domains; one of the *real-world* and one of the *systems thinking view of the real-world,* which is a conceptual view. The stages in Figure 9.1 are executed in continual iteration until the real-world is improved.

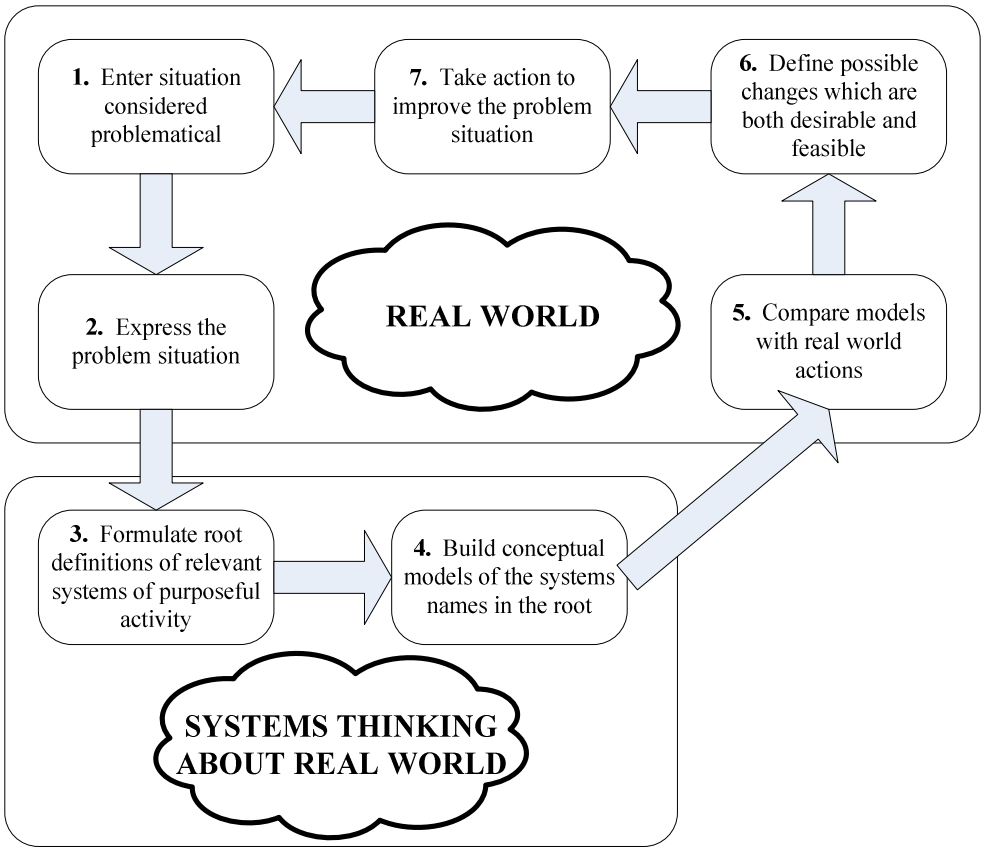

Figure 9.1: The Conventional Seven-stage Model of SSM (Checkland & Scholes, 1990, p.27)

Once the problem is better understood, the principles of hard systems theory can be applied in order to *design a system* to address the problem. However, one should be aware that there are critics that claim this linear approach to problem solving, which includes cause and effect, is incomplete. These critics promote complexity theory and advocate that human behaviour cannot be modelled and

understood in the same way as physical phenomena. However, this research project subscribes to causation, as described in Section 2.2.3, when considering that *all* decisions have consequences, even unintended consequences.

To highlight the systems thinking approach, complex systems are managed by focussing on the whole, not necessarily on parts of the system. The whole is made up of the *cause and effect of the interaction between the individual parts* (Smith & Fingar, 2003). Thus, all parts need to be focussed on enabling the core competency of the whole; in this study – *increased trust and control*. Additionally, it is not claimed that the parts are sequenced in a linear fashion in order to contribute to the whole.

In concluding this section, the argument of the soft systems approach hinges on the fact that future human behaviour cannot be predicated in the same way hard systems (natural and design systems) can be. Hard systems prescribe that, based on prior experience; the future can be predicated with a degree of accuracy, thereby reducing perceived uncertainty (using probability and likelihoods). However, without debating this notion further, this thesis incorporates elements of both soft and hard systems when addressing the problem. This is because the problem involves both design and human systems elements. A predictive cause and effect approach is applied to the problem and is illustrated in a causal model. Finally, it is acknowledged that due to the human aspects of the problem, not all solutions can be prescribed in the same manner, yet the analysis has followed a systems perspective.

9.3 CAUSALITY

This philosophical concept of causality or the principles of causes refers to the set of 'cause and effect relations'. A general definition is that, *"causality always implies at least some relationship of dependency between the cause and the effect"* (Causality, 2006). For example, deeming something a cause may imply

that if the cause occurs, the effect does as well. There are many different philosophical views on causality, sometimes referred to as causation.

One of these views of causality is termed *Necessary and Sufficient Causes*, which will now be discussed (Necessary and Sufficient Conditions, 2006). Causes are differentiated into two types: Necessary and Sufficient and the following example is used to illustrate this notion.

- *Necessary causes*: If ***x*** is a necessary cause of ***y***; then the presence of ***y*** necessarily implies that ***x*** preceded it. The presence of ***x***, however, does not imply that ***y*** will occur.
- *Sufficient causes*: If ***x*** is a sufficient cause of ***y***, then the presence of ***x*** necessarily implies the presence of ***y***. However, another cause ***z*** may alternatively cause ***y***. Thus the presence of ***y*** does not imply the presence of ***x***.

When applying necessary and sufficient causes to this research problem, the cause is identified as corporate financial scandals and substandard financial reporting. The effect is the loss of stakeholder confidence and trust. However, the notion of sufficient causes argues that the loss of stakeholder confidence and trust, could possibly be caused by another factor, in other words a different cause. Nevertheless, this research project has identified the cause as substandard financial reporting which has led to a *trust problem*: the effect.

In order to address this trust problem, it has become necessary to address the cause so as to minimise the effect. If the cause is addressed, it will affect the trust problem or explained another way, ***x*** will affect ***y***. This is in harmony with manipulation theories (Causation and Manipulability, 2006) where ***x*** causes ***y*** and one can change ***x*** in order to change ***y***. However, this philosophical view is also not without its critics, who claim one cannot manipulate causality that is essentially the relationships between parts.

To clearly position the causal model and the problem within a causal system environment, the principles of Figure 1.2 are used in Figure 9.2. This allows one to illustrate a cause and effect process within a system's perspective. It is important to note that *Inputs* would include information security management, continuous monitoring and continuous auditing. *Outputs* include continuous assurance, better decision-making and increased trust and control.

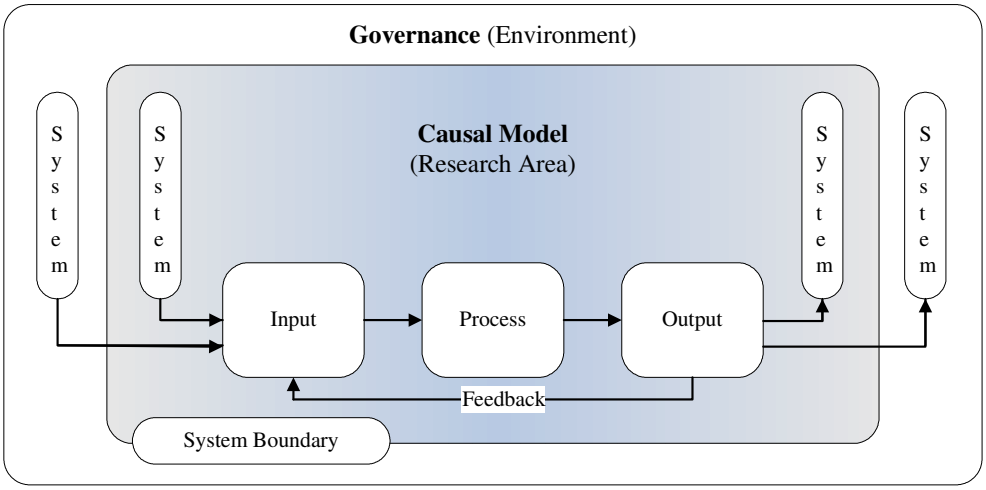

Figure 9.2: Positioning of the Causal Model

It is also important to note the *Feedback* loop from the Output box back into the Input box. This becomes an iteration process of building and safeguarding trust (see Section 3.5). It should be noted that within the System Boundary are the financial systems of a company.

It is important to highlight the linear sequence of events viewed as greed, poor morals, ethics and governance which are the cause while the effect is substandard financial reporting. However, substandard financial reporting is a cause in itself and the effect is a trust problem. Addressing the trust problem is the focus of this research project; however, one cannot address the trust problem without addressing its cause.

9.4 'PARTS' AND THE 'WHOLE' OF THE CAUSAL MODEL

There are many parts of this causal model, which together through their relationships, form a whole. These parts, or smaller wholes, are discussed throughout this thesis as sections with their own emergent properties. Some of these have formed chapters. These chapters again form parts of the whole presented as this research project, with the emergent property of *increased trust and control* within the research area of Figure 9.2. This section 9.4 conveys the whole and also discusses a few of the parts which make up the whole. It is important to note that not all sections of the model are actually parts or smaller wholes, but the model also represents inputs, process, outputs and relationships.

This causal model represents a real-world situation and focuses on both the problem and the solution, as Hevner and March (2003) have advocated models should be. It is important to view this model from the top down, starting with stakeholder mistrust and uncertainty as symptoms of the cause. These inputs are transformed by the process, as discussed in the latter parts of this chapter, into outputs of increased trust and control, including reduced uncertainty.

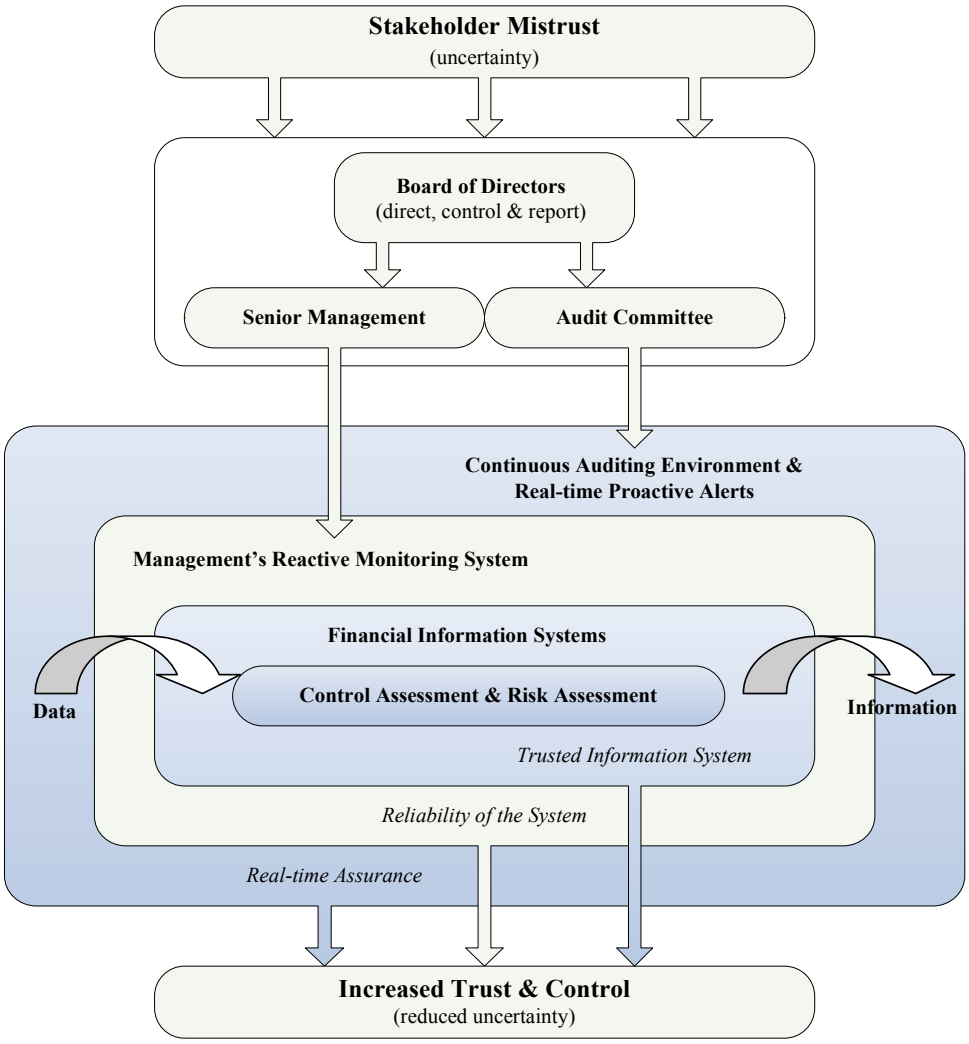

Figure 9.3: Causal Model for Increased Trust & Control

Four parts or smaller wholes of the model will now be introduced and discussed in more detail. These are graphically illustrated in Figures 9.4 – 9.7 and are highlighted by shading the boxes, so as to provide clarity when discussing them.

- The directors and executive management
- Financial information systems
- Management's monitoring system
- Continuous auditing system

9.4.1 The Directors and Executive Management

This part incorporates the board of directors, executive management and the directors who are members of the audit committee. These are discussed in Sections 2.3 and 5.4. The focus is on corporate governance, control, agency theory and the audit committee. It deliberates how, ultimately, the directors have the responsibility for managing risk, including information security and controls. This includes the integrity of the information found within the financial statements.

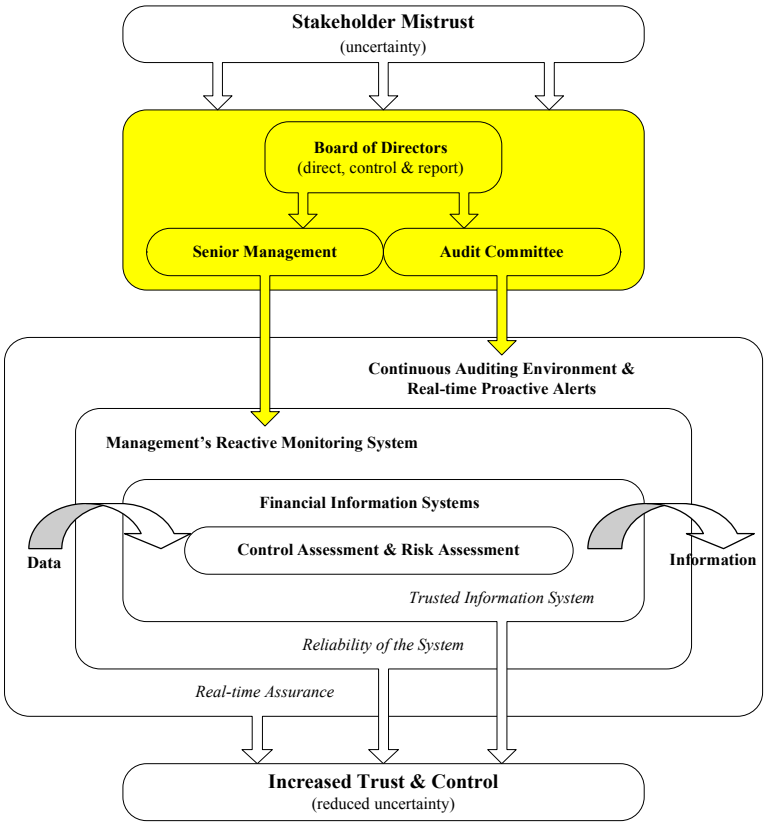

Figure 9.4: The Director's 'Part'

Suspicion and mistrust has been targeted at the directors as the stakeholders expect them to ensure that a system is in place to monitor management. Additionally, the directors can influence the company's financial statements in order to obscure the company's true financial position. As represented in Figure

5.1 and in the causal model, the directors can influence both management's monitoring system and the auditor's systems. From a *governance* and *control* perspective this is a crucial 'part' or smaller whole.

9.4.2 Financial Information Systems

Financial information systems (FIS) are the most important systems a company can have as it is these systems that capture and process the financial data and information. Management and directors base strategic decisions on the information held within these systems, which ultimately determine the company's direction and future. However, it is also these systems which are often the focus of security attacks. This is a major issue. For example, a threat breaching the security controls of a system automatically decreases the amount of trust placed in that system, as perceived risk has increased. By providing assurances that threats are contained, that controls are adequate, and that possible risks to the system are being managed appropriately, trust in the system will increase. This example clearly illustrates the cause and effect principles. The importance of information to a company is highlighted in Section 2.5 and information security in Section 2.5.2.

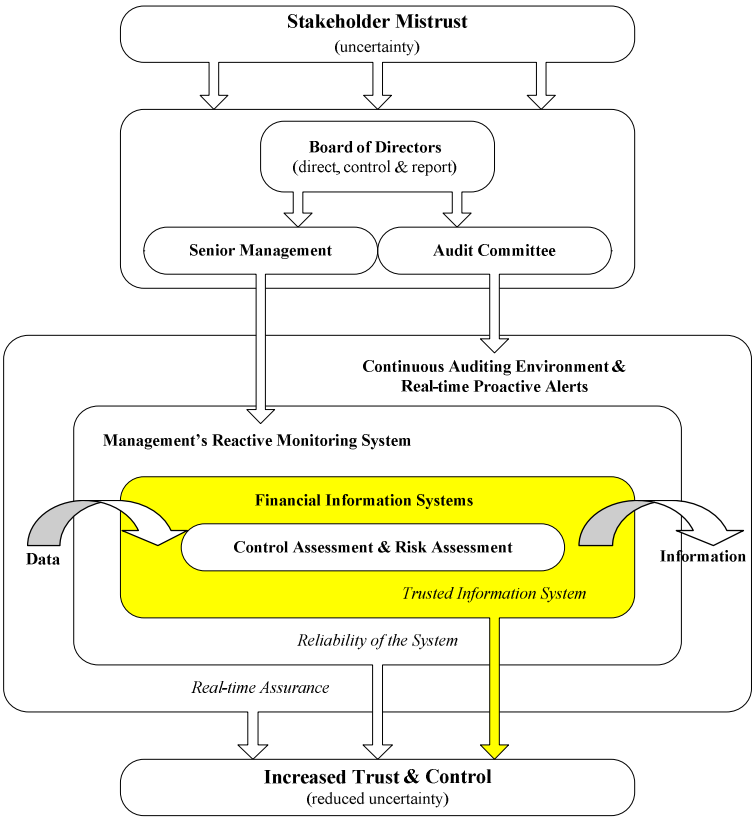

Figure 9.5: Financial Information System's 'Part'

It is these financial systems and the information found within these systems, which needs to be *trusted*. Assurances should therefore be provided in real-time for these real-time systems could indicate whether erroneous or fraudulent activity has taken place. Both control assessment and risk assessment procedures need to be applied, as discussed in Sections 5.2 and 7.3.2. An important point to take note of is that these *trusted information systems add to the overall emergent property of the whole of increased trust and control*.

9.4.3 Management's Monitoring System

It is crucial that management has a monitoring system to check if the business processes and systems for which they are responsible, are functioning properly as intended, including the system of internal controls, which incorporates IT

controls. A real-time monitoring system for management is discussed in Sections 4.4.5 and 7.2.

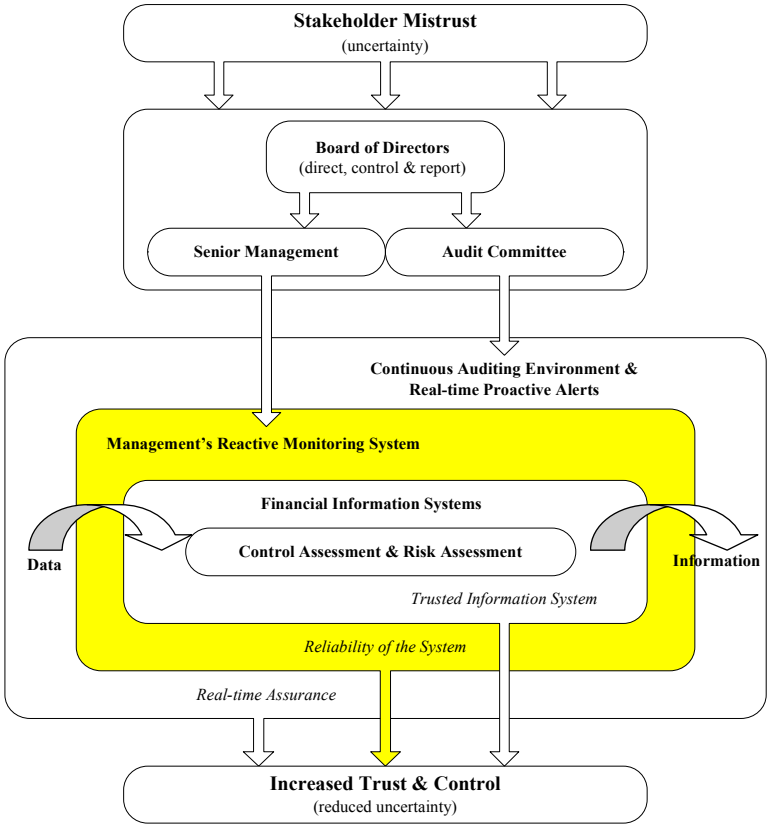

Figure 9.6: Management's Monitoring System's 'Part'

As can be noted in Figure 9.6, management's monitoring system is *reactive* by nature. The system highlights failure so that management can rectify the problem situation. Additionally, it can be noted that the arrow leading down from the director's part influences this part. Also, it surrounds the financial information systems part, as management is responsible for the integrity of FIS. Finally, it is important to note that management's monitoring system indicates the reliability of the systems monitored. *System's reliability influences trust and control which are emergent properties of the causal model as a whole.*

9.4.4 Continuous Auditing System

This thesis has discussed continuous auditing systems in-depth as a way of providing real-time assurances in an effort to address the problem. This *proactive* approach allows the decision-makers' confidence when basing their decisions on the information found within the company's financial information systems. The continuous auditing environment surrounds all the company's information systems, including management's monitoring system. This was discussed in detail in Chapters Seven and Eight.

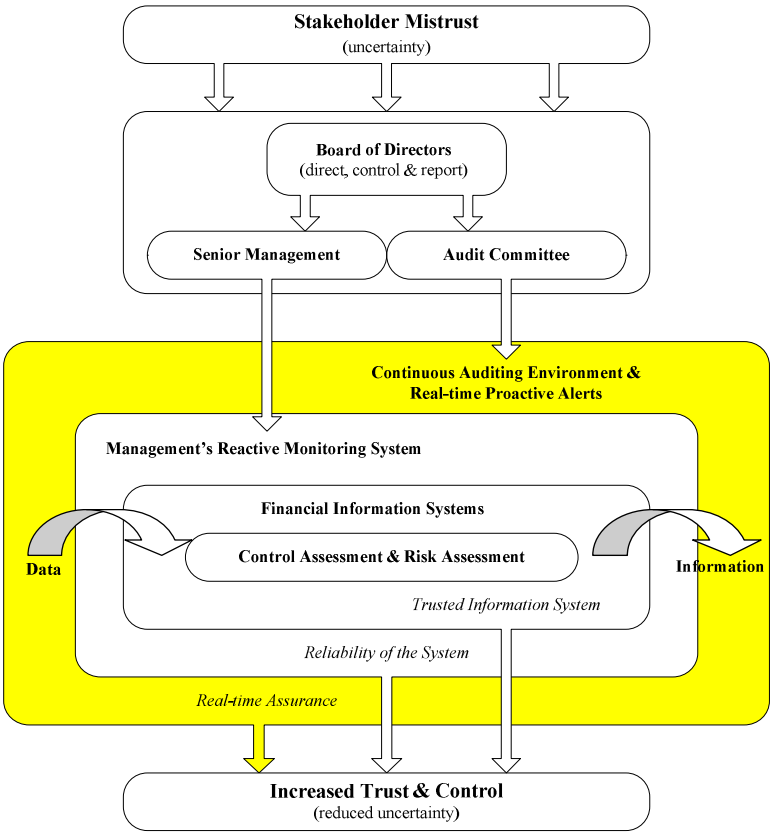

Figure 9.7: Continuous Auditing System's 'Part'

What is important to note is that continuous auditing follows the traditional audit principles; however, it allows the auditor to provide assurances in real-time. These real-time independent assurances permit trust to grow, as discussed in the Stag Hunt (also known as the Assurance Game - Section 3.3.3). *Continuous*

auditing is a crucial part of the whole and the whole's emergent property of increased trust and control.

9.5 CONCLUSION

There is one problem with two interrelated and interdependent parts, which were addressed in this thesis and by the causal model. Firstly, *lack of financial information integrity* within the company's financial statements, leads to the second part of the problem, which is a *trust problem.* To address the first part affects the second.

The causal model requires Stakeholder Mistrust and Uncertainty to be inputs at the top of the model, while the main focus in the middle of the model addresses the financial information. The financial data is inputted on the left of the model, processed and then information with integrity is an output on the right.

However, the two parts of the problem converge in the centre of the model and become the focus, as they are addressed simultaneously. The outputs are increased trust and control on the bottom, because the information has been verified by a continuous auditing process and information integrity is therefore established.

Chapter 10

CONCLUSION

"A theory, ultimately, must be judged for its accord with reality."
- Stanislaw Leshniewski, (mathematician and scientist, 1886 - 1939)

10.1 MILIEU

This study researched how to restore stakeholder confidence and trust in boards of directors in the domain of financial reporting with specific emphasis on information and the integrity thereof. To accomplish this, various topics, including governance, trust, risk, auditing and assurances were examined in order to understand how to reduce uncertainty and restore trust. The procedure of determining if information has integrity was scrutinised and recommendations made. Finally, a continuous auditing process was proposed with its foundations grounded in information technology.

It was argued that the key to addressing the research problem is to provide assurances in real-time. This is because decisions are made in real-time and are based upon real-time information. The core of this concluding chapter evaluates whether the research objectives were met. Following this, the study's limitations and areas for future research are discussed.

10.2 EVALUATION OF THE RESEARCH OUTCOMES

The primary objective of this study was to produce a causal model, which will result in increasing stakeholder confidence and trust in the domain of financial

reporting. In order to achieve the primary objective, a number of secondary objectives were addressed. This was done in line with systems theory, where the 'parts' together constitute the 'whole'. The whole then had an emergent property, which addresses the problem. The remainder of this section addresses the secondary objectives or the parts of the problem, which were identified in the introductory chapter, Section 1.4.

Research Objective: *A study of the theories and processes underlying corporate governance and the causes of corporate financial scandals.*
This objective was discussed in detail in Chapter two. An important ingredient of this objective is to understand the principles and causes or the root of the problem in order to focus this research project. This then avoids the error of addressing the symptoms and effects of the problem.

To have good governance, companies need efficient structures, defining the relationship between the board of directors, management and other stakeholders. Moreover, assurances need to be offered to investors that their money is being used wisely to avoid adverse reactions. The crucial roles the directors play in the governance of companies are taken into account and include power, accountability and responsibility. The principles of Agency Theory were discussed. These revolve around the company issue of ownership and control, including conflict of interest, which directors confront when they direct and control a company.

The corporate financial collapses and scandals highlight that some directors are weak and ineffective monitors of managers. This board 'weakness' has called for additional mechanisms for monitoring and controlling of management. This has led to the plethora of codes that companies and directors need to comply with in order to help restore stakeholder, especially investor, confidence.

An important issue that has come to the fore as a result of these corporate debacles is that the information assets of a company need to be protected and

secured. Directors cannot effectively lead and guide the company if they do not have real-time accurate and reliable information, or at least have knowledge as to the 'condition' of the information. In addition, investors may easily be misled for the same reason. All stakeholders, including directors and investors, need to have assurances that the information on which they base their decisions, is both reliable and accurate. This requires greater transparency in the makeup of financial statements, including the system of controls, which leads to the development of uncertainty reduction and the establishment of trust.

The findings of this objective stressed the importance of Agency Theory and that directors have not always practiced good governance. As a result many 'codes' have been introduced that companies and directors need to comply with. These regulatory codes stress the importance of sound financial reporting and the protection of information assets. This is done in order to restore stakeholder, especially investor, confidence and trust in a board of directors in the financial reporting domain. These findings clearly illustrate that this research objective has been met.

Research Objective: *An investigation into the various trust theories and the relationship trust has with uncertainty, risk and behaviour.*
This objective helped to understand this complex subject and how the restoration of trust can occur. One first has to build trust, and then, because of the fragile nature of trust, one needs to safeguard it in order not to 'lose' it again. It was established that mutual assurances assist in building trust and that information security assists in safeguarding trust.

In line with this form of reasoning, it is important to note that directors should be perceived as trustworthy. To be considered trustworthy, three elements are required: Integrity, Benevolence and Ability. Furthermore, once trustworthiness is established, the relationship that trust has with risk needs to be taken into account, as this relationship will have an effect on behaviour. However, one also needs to note that in order to have confidence in one's decisions, it is important

to be aware that confidence consists of two elements: trust and control. Both absolute trust and absolute control are extremes of the pendulum, and one needs to find the right balance between the two. This is based on the understanding that trust can evolve and grow by providing positive assurances; however, information security, which includes controls, is required to safeguard trust, once established.

As noted, this research objective was to investigate various trust theories and the relationship trust has with uncertainty, risk and behaviour. The relationships have been established, and richly debated. Moreover, if the principles of the Stag Hunt (Assurance Game) are taken into account, the assurances need to be provided in real-time as ex-post assurances are insufficient, and the level of uncertainty will be high until assurances are provided. So, in order to have a positive relationship and to avoid unfavourable behaviour, uncertainty needs to be contained, and the level of trust needs to surpass the perceived risks. To follow on from this, one cannot escape that trust and controls affect confidence and are the reason for the acceptance of a degree of insecurity. Accordingly, this research objective concluded that confidence in information security requires trust and trust requires information security to help safeguard it.

Research Objective: *Determining the role of the audit committee, the function of internal controls relating to financial statements and information security.*
This study addressed the issue that risk is intrinsic to governance and to address one of these areas is to simultaneously affect the other. However, this study went further and highlighted that trust and risk are significant variables and when one is addressed, the other is affected. This cause and effect principle was referred to throughout this thesis.

An important sub-committee of a board, the audit committee, helps provide assurances that the financial statements are a fair presentation of the company. This important committee is there to assist both the *Agents* and the *Principals*. The Agents receive assurances from the audit committee that management's risk

practices, including a system of internal controls, are effective and efficient and therefore, the company's risk exposure is adequately addressed. The Principals receive assurances that the directors are governing the company in an appropriate manner and that the financial statements reflect the 'true' condition of the company.

The governance principles of accountability, responsibility, transparency and fairness are principles addressed by an audit committee and auditors. These parties help to ensure that the information within the financial statements is both accurate and reliable. When assurances are provided, trust between the various parties can grow and uncertainty will be reduced, as the perceived risk will have been reduced, as with the hunters during the Stag Hunt. This objective considers how auditors *validate the accuracy* of the financial information. However, the auditors also *validate the reliability* of the system of internal controls. The auditors, reporting to the audit committee, then become an independent source of information and a source of trust.

Evidence collected when addressing this research objective highlighted that the auditing profession needs to keep pace with technological change and the fast pace of business. Providing assurance months after transactions have occurred is insufficient. Real-time assurances are required. This is where an audit committee fulfils a crucial function in providing a monitoring role and establishing good governance. This subcommittee of a board of directors is responsible for the *risk management*, *financial reporting* and *the audit function*. Consequently, this committee allows the Principals some degree of 'security' in knowing that the risks (both direct and indirect) the company is exposed to are being managed effectively and that the Agents are not conspiring against them.

Research Objective: *Determining the elements of what constitutes information integrity and assurances specifically within the domain of financial statements.*
Determining if information has integrity is not to be taken lightly and is not a straightforward task. En route to determining if information has integrity, of

which there will only be reasonable assurances provided, one first has to determine if the *data* has integrity. One cannot move into information integrity without going through a process of checking if the foundation of information, data, is quality data and retains its integrity. Additionally, one cannot decide on data alone to verify information integrity. It is necessary to check if the *system* that processes the data has integrity. For a system to have integrity and to be reliable, an adequate system of internal controls is required to ensure the security of the system. Therefore, it is important to consider the integrity of each step in the linear sequence of when data processed becomes information and information interpreted becomes knowledge. As discussed in Section 6.3.1, to have quality decisions, one needs quality information.

The elements of information integrity are clearly illustrated in Figure 6.7, Information Integrity Attributes, and have been discussed in detail in Chapter Six. However, to meet the second part of this research objective of how to provide information assurance was to address the fact that information can be no better than the integrity of the system processing the data, although it can be worse. In addition, if the data lacks integrity at the time it enters the system, then the data will continue to lack integrity when it is transformed and processed into an output of the system.

This objective contributed to the thesis in that it highlights that in practising good governance, directors need to ensure that the information within their company's financial information systems is sound and has its integrity intact. Moreover, to restore confidence and trust between the various company stakeholders, the directors need to ensure that the financial statements have integrity. This leads towards building trust and restoring investor confidence within the financial domain.

Two Research Objectives Addressed Simultaneously: *Identifying attributes of a company suggesting that a continuous auditing process is appropriate, including technologies available. At the same time, addressing whether the*

continuous auditing models will assist in verifying financial information integrity in real-time and thereby provide assurances on demand. These objectives were discussed in detail in Chapters Seven and Eight.

As noted, there are various technologies available and continuous auditing models proposed that will assist a company in setting up a continuous auditing process. Technologies, such as Extensible Business Reporting Language, Embedded Audit Models, Data Warehousing, Data Mining, Business Intelligence and Artificial Intelligence, are accessible to companies today. It is merely a matter of companies using these technologies together in order to verify information, as suggested by the models in Chapter Eight.

These technologies address both the identification of control deficiencies, which highlight areas of potential risk and conversely, the examination of risk through analytical procedures, such as trend analysis, which identify areas where controls are inadequate. Chapter Seven has addressed *what* continuous auditing is and what technologies can be used to play a part in the continuous auditing process. However, Chapter Eight built on this and addressed *how* continuous auditing can be performed as three of the better-known models were critically discussed and compared.

Chapter Eight's comparison of three influential continuous auditing models highlighted a lack of consensus on the technologies used to address this challenge, and on how a continuous auditing system should function. However, these models each contribute to solving the problem of providing assurances in real-time rather than months after the transactions have occurred. But importantly, they all attempt to address the challenge of *standardisation of data* to enable effective analysis, the validation of the *accuracy of the financial data* and the *reliability of the system,* which processes and houses the financial data and information. Onions' model, A Proposed Model for Secure Continuous Auditing, is being tested at Rutgers University - CARLAB laboratory in the USA, where they have accumulated data from six different companies for a five-

year period. These researchers analyse transaction patterns and run tests in an attempt to improve the model and increase the effectiveness of continuous auditing (personal communication, Robert Onions, September 2006).

These two objectives have been met and contributed to the overall research project in that they demonstrate that real-time financial assurances can be produced, thereby allowing the various stakeholders confidence when basing their decisions on real-time financial information. The information becomes more trustworthy as the auditing and assurance principles are applied in real-time. Additionally, this allows for better decision-making. Trust can grow in real-time, as in the Stag Hunt, and assurances are provided as to the integrity of the information, in real-time.

One can confidently state that these secondary objectives, or 'parts' of the 'whole', have been discussed and met. However, though they may be individually inadequate to address the research problem, collectively they are adequate. The argument that trust and control, the emergent properties of the secondary objectives, can help restore stakeholder confidence and trust in the board of directors is rational.

10.3 LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

This section discussed some limitations of this study followed by areas for future research. This study proposed a conceptual model based on a theoretical argument, extracted from literature, where no empirical research has been conducted. The argument line and chosen literature were influenced by the researcher's perceptions. This had inherent difficulties when attempting to recommend objective solutions.

It is acknowledged that the research problem could have been addressed in different ways by different researchers. However, every attempt has been made to examine the subject from different viewpoints and to choose the most

appropriate literature and topics when addressing the problem. This has been guided by systems theory, where the 'parts' chosen contribute to the 'whole'. The emergent property of the whole addressed the research problem of - *trust and control*. It was argued that continuous auditing can provide increased trust and control.

A study of this magnitude, which has drawn on many different disciplines and research areas, cannot capture all the views on the relevant topics and therefore, there is room for future research. Although the study has tried to address many important issues, the following two aspects should be clarified.

Firstly, the relationship between trust, controls and confidence is an important issue. Figures 3.3 and 4.1 graphically illustrate this relationship as constant, with a straight line between trust and control. However, there is a strong likelihood that this line is not as straight, as shown in these figures. Therefore, there is the probability that the line is curved, and the relationship between trust and control is not perfectly constant. The relationship should consider more factors and be interrogated as game theory has been over the years.

Secondly, the method chosen to restore confidence and trust between company stakeholders is continuous auditing. Technologies are available for this process; however, they have not been proven to work together. Future research could embark on an engineering project to build and test these models in the hope that industry and the auditing profession will embrace this new process in order to provide real-time assurances.

10.4 EPILOGUE

This thesis presented a study where assurances need to be provided in real-time to restore stakeholder confidence and trust in the domain of financial reporting. The comparison to the Stag Hunt cannot be emphasised enough. In the Stag Hunt, the hunters continuously communicate with each other in order for the

hunt to be successful. They provide mutual assurances that they are committed to the hunt. If the uncertainty levels are too high during the hunt, the hunters may choose to defect and hunt rabbit, and the stag hunt will collapse. Trust needs to exist between the hunters for their hunt to be successful.

In the same manner, directors communicate with the company's stakeholders, especially investors, via a company's financial statements. Assurances need to be provided in real-time that the information found within company financial systems has integrity. Also, are the company's risks contained? Is the company on course, as intended, and are the intentional and unintentional errors within the financial statements limited? If not, a trust problem occurs. The solution is to provide independent real-time assurances, via continuous auditing, when the information becomes available, and not months later, as is the case with traditional auditing.

REFERENCES

582 weakness, deficiency disclosures made in '04. (2005, January 11). *Compliance Week*. Retrieved January 11, 2005, from http://www.complianceweek.com/index.cfm?fuseaction=article.viewArticle&article_ID=1456

AAIA. (2006) American Association for Artificial Intelligence. Retrieved July 7, 2006, from Website http://www.aaai.org

A Question of Accountability. (2002, June 16). *The New York Times*, section BU12.

Abrams, L. C., Cross, R., Lesser, E., & Levin, D. Z. (2003). Nurturing Interpersonal Trust in Knowledge-sharing Networks. *Academy of Management Executive*, 17(4), 64 – 77.

Abdolmohammadi, M. J., & Sharbatouglie, A. (2005). *Continuous Auditing: An Operational Model for Internal Auditors*. Florida, USA: The Institute of Internal Auditors Research Foundation.

ACPET. (2006, February). Audit and Risk Committee Terms of Reference, Australian Council for Private Education and Training. Retrieved, 2006, February 16, from http://www.acpet.edu.au/corporate/audit_committee_terms_of_reference3

AICPA. (1997). *The Information Technology Age: Evidential Matter in the Electronic Environment*. AICPA, New York: USA.

AICPA, & CICA. (1999). *SysTrust Principles and Criteria*. American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. USA & Canada.

AICPA. (2002). The Business Reporting Model of the Future. American Institute of Certified Public Accountants. Retrieved March 23, 2005 from http://www.aicpa.org/pubs/cpaltr/nov2002/supps/edu1.htm

AICPA. (2005). *2005 Top Technologies Survey.* The American Institute of Certified Public Accountants. Retrieved June 9, 2005, from http://www.aicpa.org/download/news/2005_0103.pdf.

Allen, J. (2005). Governing for Enterprise Security. Networked Systems Survivability Program. USA: Carnegie Mellon University.

Alles, M., Kogan, A., & Vasarhelyi, M. (2005). *Real time reporting and assurance: Has its time come?* Retrieved February 4, 2005, from Rutgers Business School, Web site: http://raw.rutgers.edu/continuousauditing/

Amplitude Research. (2005, February 15) Viruses and Worms Top Security Threat List. Retrieved January 14, 2006, from http://www2.cio.com/metrics/2005/metric770.html

Applegate, D. & Wills, T. (1999). Struggling to incorporate the COSO recommendations into your audit process? *Internal Auditor,* December, Retrieved September 10, 2004, from http://www.coso.org/audit_shop.htm

Arens, A. A., Elder, R. J., & Beasley, M. S. (2003). *Auditing and Assurance Services* (9th Ed.). New Jersey: Pearson Education, Inc.

Australian Government. (2001). Information Management Office: Glossary. Retrieved May 19, 2005, from http://www.agimo.gov.au/publications/2001/11/ar00-01/glossary.

Axelrod, R. (1997). *The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration.* New Jersey: Princeton University Press.

Axelrod, R. (1984). *The Evolution of Cooperation.* New York: Basic Books.

Bai, C., Liu, Q., Lu, J., Song, F. M., & Zhang, J. (2004). *Corporate Governance and Market Valuations in China*. Retrieved May 16, 2005, from http://www.hiebs.hku.hk/working_paper_updates/pdf/wp1096.pdf

Barquin, R. (2000) From Bits and Bytes to Knowledge Management. Retrieved May 9th, 2006, from Website: http://www.barquin.com/

Basel II Accord. (2004). *The New Basel Capital Accord*. Basel Committee on Banking Supervision. Switzerland: Bank for International Settlements.

Bassey, M. (1999). *Case Study Research in Educational Settings*. UK: Open University Press.

Bavoso, P. (2002). Is Mistrust Holding Back Supply-Chain Efforts? *Optimize, and InformationWeek Resource*. Retrieved May 8, 2003, from http://www.optimizemag.com/printer/014/pr_squareoff_yes.html.

Becht, M., Bolton, P., & Roell, A. A. (2002). *Corporate Governance and Control*. Retrieved May 12, 2005, from European Corporate Governance Institute – Finance Working Paper No. 02/2002, Web site: http://www.ecgi.org/codes/all_codes.php

Berger, C. R., & Calabrese, R. J. (1975). Some Explorations in Initial Interaction and Beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research*, 1, 99-112.

Berger, C. R. (1987). Communicating Under Uncertainty. In M. Roloff & G. Miller (Eds.). *Interpersonal Processes: New directions in communication research*. 39-62. California, USA: Sage Publications

Berle, A. A., & Means, G. C. (1967). *The Modern Corporation and Private Property*. New York: Harcourt, Brace & World.

Bierstaker, J. L., Burnaby, P., & Thibodeau, J. (2001). The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. *Managerial Auditing Journal*, 16 (3), 159-164.

Bierstaker, J. L., Burnaby, P., & Hass, S. (2004). Recent Changes in Internal Auditors' use of Technology. *Internal Auditing*, 18(4), 39-45.

Bletner, C. S. (n.d.) Operational Risk Management. U.S. Navy (vr-53). Retrieved July 14, 2005, from www.cdc.gov/niosh/sbw/posters/pdfs/**bletner**.pdf

Boritz, J. E. (2005). IS Practitioners' Views on Core Concepts of Information Integrity. *International Journal of Accounting Information Systems*, 6, 260-279.

Bovee, M. W. (2004). Information Quality: A Conceptual Framework and Empirical Validation. Retrieved December 9, 2005, from http://www.bsad.uvm.edu/Research/FacPubs/details?author=265

Bovee, M., Srivastava, R. P., & Mak, B. (2003). A Conceptual Framework and Belief-function Approach to Assessing Overall Information Quality. *International Journal of Intelligent Systems*, 18(1), 51-74.

Bradshaw, P., & Jackson P. (2001). *Loyal Opposition*. Retrieved April 19, 2005, from http://www.camagazine.com/index.cfm/ci_id/6608/la_id/1.htm

Braiotta, Jr., L. (2002). Corporate Audit Committees: An Approach to Continuous Improvement. *CPA Journal,* 73 (2).

Braun, R. L. & Davis H. E. (2003) Computer-assisted audit tools and techniques: analysis and perspectives. *Managerial Auditing Journal*, 18 (9), 725-731.

Bribery in Russia Shoots up. (2005, July 22). *Finance24.com*. Retrieved July 23, 2005 from http://www.finance24.com/articles/default/display_article.asp?Nav=ns&ArticleID=1518-1786_1741959

British East India Company. *Wikipedia, the free encyclopaedia*. Retrieved June 22, 2005, from http://en.wikipedia.org/wiki/British_East_India_Company

Brush, M. (2005, September 16). The 5 outrageously overpaid CEOs. MSN Money. Retrieved September 16, 2005, from http://moneycentral.msn.com/content/P125120.asp

Budnitz, M. E. (1990). Business reorganizations and shareholders meetings: Will the meeting please come to order, or should the meeting be cancelled altogether? *The George Washington Law Review,* 58, 1214-1267.

Cadbury, A. (2002). *Corporate Governance and Chairmanship: A Personal View*. USA: Oxford University Press.

Camp, L. J. (2000). *Trust and Risk in Internet Commerce.* England: The MIT Press.

Camp, L. J. (2002). Designing for Trust. In R. Falcone, S. Barber, L. Korba, M. Singh (Eds.). *Trust, Reputation, and Security: Theories and Practice*. 15-29. Berlin: Springer-Verlag.

Cangemi, M. P. & Singleton, T. (2003). *Managing the Audit Function: A corporate audit department procedures guide* (3rd Ed.). New Jersey: John Wiley & Sons, Inc.

Carlson, T. (2001). Information Security Management: Understanding ISO 17799. *Lucent Technologies Worldwide Services*. Retrieved February 1, 2004, from http://www.netbotz.com/library/ISO_17799.pdf.

Carpenter, R. N. (1988). Corporate governance, part II: Directors responsibilities, *Directors & Boards*, 29 (3), 3-6.

Causality. (2006). Wikipedia: The Free Encyclopaedia. Retrieved October 16, 2006, from *http://en.wikipedia.org/wiki/Causality*

Causation and Manipulability. (2006). Stanford Encyclopaedia of Philosophy. Retrieved October 16, 2006, from *http://plato.stanford.edu/entries/causation-mani/*

CCRC (n.d.) Computer Crime Research Centre. How Pervasive is Cyber-Crime? Retrieved 4, 2006, from http://www.crime-research.org/library/Advisor.htm

Cerullo, M. V, & Cerullo, M. J. (2004). How the New Standards and Regulations Affect an Auditor's Assessment of Compliance With Internal Controls. Retrieved May 19, 2006, from http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=26156&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Cerullo, M. J. & Cerullo, M. V. (2006). Using Neural Network Software as a Forensic Accounting Tool. Information Systems Control Journal, Retrieved March 29, 2006, from https://www.isaca.org/Template.cfm?Section=Home&Template=/MembersOnly.cfm&ContentID=24699

Chapman, C. (2001). The Big Picture – Enterprise risk management services, *Internal Auditor*, 58(3) June, 30-37.

Champlain, J. J. (2003) *Auditing Information Systems*. New Jersey: USA, John Wiely & Sons. Inc.

Charan, R., & Useem, J. (2002). *Why Companies Fail*. Retrieved May 19, 2005, from http://www2.una.edu/sborah/Prinman/why_companies_fail.htm

Checkland, P. (1999). *Systems Thinking, Systems Practice*. West Sussex, England: John Wiley & Sons, Ltd.

Checkland, P. & Scholes, J. (1990). *Soft Systems Methodology In Action.* Chichester, England: John Wiley & Sons, Ltd.

Chia, R. (2002). The Production of Management Knowledge: Philosophical Underpinnings of research design. In D. Partington (Ed.). Essential skills for management research. London, UK: Sage Publications Ltd.

CICA & AICPA. (1999). *Continuous Auditing: Research Report*. The Canadian Institute of Chartered Accountants. Canada: Ontario.

Clarke, T. (Ed.). (2004). *Theories of Corporate Governance*. USA & Canada: Routledge.

CobiT. (2000). Control Objectives for Information and Related Technology. (3rd Ed.). USA: IT Governance Institute.

CobiT. (2005). Control Objectives for Information and Related Technology. (4th Ed.). USA: IT Governance Institute.

Collis, J. & Hussey, R. (2003). *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*. (2nd Ed.).London, UK: Palgrave Macmillan Ltd.

Common Criteria. (2004). *For Information Technology Security Evaluation: Part 1: Introduction and General Model*, (version 2.2 CCIMB). Retrieved January 9,2005, from http://www.commoncriteriaportal.org/public/files/ccpart1v2.2.pdf.

Conner, B., Noonan, T., & Holleyman, II. R. W. (2004). Information Security Governance: Toward a Framework for Action. *Business Software Alliance*. Retrieved November 11, 2004, from http://www.bsa.org/resources/upload/Information-Security-Governance-Toward-A-Framework-for-Action.pdf.

Conner, F. W., & Coviello, A. W. (2004). Information Security Governance: A Call to Action, *The Corporate Governance Task Force.* Retrieved October 9, 2004, from http://www.cyberpartnership.org/InfoSecGov4_04.pdf.

Cornwell, R. (2002, July 1). Interview: Professor JK Galbraith. *The Independent*. Retrieved 16 May 16, 2004, from http://www.btinternet.com/~pae_news/GalbraithInterview.htm

Corruption costs Africa $148bn. (2006, February, 23). Retrieved February 24, 2006, from Finance24.com web site: http://www.fin24.co.za/articles/email_article.asp?articleid=1518-25_1887234

COSO-ERM. (2004). *Enterprise risk management-integrated framework.* The Committee of Sponsoring Organizations of the Treadway Commission. USA: AICPA.

COSO-ICF. (1992). *Internal Control – Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission. USA: AICPA.

Cox, R., & Marriott, I. (2003). Trust and Control: The Key to Optimal Outsourcing Relationships. Retrieved March 19, 2004, from Gartner database.

Daigle, R. J., & Lampe, J. C. (2003). Responding to the Sarbanes-Oxley Act with continuous online assurance, *Internal Auditing*, 18 (2), 3-7.

Dalal, C. (1999). Using an Expert System in an Audit: A Case Study of Fraud Detection. *IT Audit*, 2. Retrieved April 22, 2004, from http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=57

Dang van Mien, A., & Green-Armytage, J. (2002). Moving to Transaction Incident Management for IS Security. Retrieved July 28, 2004, from Gartner database.

David, J. S., & Steinbart, P. J. (2000). *Data Warehousing and Data Mining: Opportunities for Internal Auditors*. Florida, USA: The Institute of Internal Auditors.

DeMaio, H. B. (2001). *B2B and Beyond: New Business Models Built on Trust*. USA: John Wiley & Sons, Inc.

Deutsche Bank AG. (2004, July) Terms of Reference for the Risk Committee of the Supervisory Board. Retrieved February 16, 2006, from http://www.deutsche-bank.de/ir/pdfs/GO_Risikoausschuss_29_07_04_EN.pdf

DeZoort, F. (1997). An investigation of audit committees' oversight responsibilities. *Abacus,* 33 (2), 208-227.

Donaldson, W. H. (2005, January 25). *U.S. Capital markets in the post-Sarbanes-Oxley world: Why our markets should matter to foreign issuers*.

Speech by the SEC staff: London School of Economics and Political Science.

Dull, R. B. & Tegarden, D. P. (2004). Using Control Charts to Monitor Financial Reporting of Public Companies, *International Journal of Accounting Information Systems*, 5, 109-127

Dunlavy, C. A. (2004). From Citizens to Plutocrats: 19th-Century Shareholder Voting Rights and Theories of the Corporation. In K. Lipartito & D. B. Sicilia (Eds.). *Constructing Corporate America: History, Politics, Culture* (pp. 66-93). Oxford: Oxford University Press.

Dutch East India Company. *Wikipedia, the free encyclopaedia*. Retrieved June 22, 2005, from http://en.wikipedia.org/wiki/Dutch_East_India_Company

ECGI (n.d.) European Corporate Governance Institute. Website http://www.ecgi.org/codes/all_codes.php

Einstein, A. (1961). *Relativity: The Special and the General Theory*. New York: Three Rivers Press.

Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *Academy of Management Review*, 14 (1), 57-60.

Emery, M. (2004). Monitoring Sarbanes-Oxley Act: Section 409 Compliance, 2020 Governance AB, Stockholm, Sweden.

English, L. P. (1999). *Improving Data Warehouse and Business Information Quality*. New York: John Wiley and Sons.

FASB. (2005, June 1st) Minutes of the May 25, 2005 Board Meeting: Conceptual Framework. Retrieved February 19, 2006, from http://www.fasb.org/project/conceptual_framework.shtml

Feldman, A. (2005) Surviving Sarbanes-Oxley. *Inc.Com*. Retrieved February 2, 2006, from http://www.inc.com/magazine/20050901/surviving-so.html

Firestone, J. M., & McElroy, M. W. (2003) *Key Issues in the New Knowledge Management.* USA:Butterworth-Heninemann

Fisher, C. W. & Kingma, B. R. (2001). Criticality of Data Quality as exemplified in two Disasters. *Information & Management*, 39(2), 109-116.

Fleckenstein, B. (2005, April 4). Dear CEOs: Stop fudging your numbers. *MSN Money*. Retrieved September 16, 2005, from http://moneycentral.msn.com/content/P113088.asp?

Fleischer, V. (2006, January 24) Is SOX leading more firms to go private? Conglomerate: Business Law Economics Society. Retrieved February 2, 2006 from http://www.theconglomerate.org/2006/01/is_sox_leading_.html

Flood, R. L. & Jackson, M. C. (1991). *Creative Problem Solving: Total System Intervention*. Chichester, England: John Wiley & Sons, Ltd.

Flowerday, S., & Von Solms, R. (2005a). Real-time Information Integrity = System Integrity + Data Integrity + Continuous Assurances. *Computers & Security*, 24(8), 604-613.

Flowerday, S., & Von Solms, R. (2005b). Continuous Auditing: Verifying Information Integrity and Providing Assurances for Financial Reports. *Computer Fraud & Security*, 7, 12-16.

Flowerday, S., & Von Solms, R. (2006). Trust: an Element of Information Security. Presented at IFIP/SEC 2006, Karlstad, Sweden. Published in S. Fischer-Hubner, K. Rannenberg, L. Yngstrom, S. Lindskog (Eds.). Security and Privacy in Dynamic Environments. 87-98. IFIP. USA: Springer.

Flowerday, S., Blundell, A., & Von Solms, R. (2006). Continuous Auditing Technologies and Models: A discussion. *Computers & Security, 25*(5), 325-331.

Free Financial Dictionary (n.d.) Falex - *Due Diligence.* Retrieved October 9, 2005, from http://financial-ictionary.thefreedictionary.com/Due+Diligence+-+DD

Free Legal Dictionary (n.d.) Falex *Due Care*. Retrieved October 9, 2005 from http://www.thefreedictionary.com/due%20care

Freedom of Information Centre (2002, September 13). Arthur Andersen Verdict Upheld. *The Associated Press*. New York. Retrieved April 12, 2005, from http://foi.missouri.edu/enronandetal/aaverdictupheld.html.

Fukuyama, F. (1996). *Trust: The Social Virtues and The Creation Of Prosperity*. New York: Free Press.

Garai, G. Mason, E. Levinson, G. & Thompson, S. (2005) SOX Impact on M&A/Financing Transactions. Retrieved January 14, 2006 from www.foley.com/files/tbl_s31Publications/FileUpload137/2689/NDI_SOXMandA_final.pdf

Gefen, D., Rao, V. S., & Tractinsky, N. (2002). The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarification. *Proceedings of the 36th Hawaii International Conference on System Sciences. IEEE Computer Society.* Retrieved March 9, 2005, from

http://csdl.computer.org/comp/proceedings/hicss/2003/1874/07/187470192b.pdf.

Gerber, M., & Von Solms, R. (2005). Management of Risk in the Information Age. *Computers & Security* 24, 16-30.

Gerck, E. (2002). *End-To-End IT Security*. Retrieved October 16, 2004, from http://www.nma.com/papers/e2e-security.htm

Gilbert, W. J. (2006). *Sarbanes-Oxley for Dummies*. Indianapolis, USA: Wiley Publishing, Inc.

Greenspan, A. (2002). *Testimony of Chairman Alan Greenspan*. Federal Reserve Board's semi-annual monetary policy report to the Congress. Retrieved April 16, 2005, from http://www.federalreserve.gov/boarddocs/hh/2002/july/testimony.htm

Greenstein, M., & Vasarhelyi, M. (2002). *Electronic Commerce: Security, Risk, Management and Control* (2nd Ed.). New York: McGraw-Hill.

Groomer, S. M., & Murthy, U. S. (1989). Continuous auditing of database applications: An embedded audit module approach, *Journal of Information Systems (spring)*, 53-69.

GTAG1. (2005). *Global Technology Audit Guide: Information Technology Controls*. USA: The Institute of Internal Auditors.

GTAG3. (2005). *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*. USA: The Institute of Internal Auditors.

Gudykunst, W.B. (1985). A Model of Uncertainty Reduction in Intercultural Encounters. *Journal of Language and Social Psychology,* 4, 79-97.

Hagel, J., & Seely Brown, J. (2002). Control vs. Trust – Mastering a Different Management Approach. Retrieved September 16, 2005, from www.johnhagel.com/paper_control.pdf

Handfield, R. B., & Nichols Jr., E. L. (2002). *Supply Chain Redesign: Transforming Supply Chains into Integrated Value Systems.* New Jersey: Financial Times Prentice Hall.

Hanson, B. G. (1995). *General Systems Theory Beginning with Wholes*. Washington, D.C.: Taylor & Francis.

Hayes, F. (2005). Is Game Theory Useful for the Analysis and Understanding of Decision Making in Economic Settings? Retrieved April 2, 2005, from http://www.maths.tcd.ie/local/JUNK/econrev/ser/html/game.html.

Helms, G. & Mancino J. (1999). The CPA & the Computer: Information Technology Issues for the Attest, and Assurance Services Functions. *The CPA Journal*. Retrieved May 16, 2005, from http://www.nysscpa.org/cpajournal/1999/0599/departments/cpac.html

Hevner, A. R. & March, S. T. (2003). The Information Systems Research Cycle. *IT Systems Perspectives,* 11, 111-113. Web site http//doi.ieeecomputersociety.org

Hodge, N. (2002). *Wall Street broker rebuked for misleading investors*. Retrieved July 11, 2005, from World Socialist Web Site: http://www.wsws.org/articles/2002/june2002/merr-j05_prn.shtml

Horton, T. R., Le Grand, C. H., Murray, W. H., Ozier, W. J., & Parker, D. B. (2000). *Information Security Management and Assurance: A Call to Action*

for Corporate Governance. The Institute of Internal Auditors: Retrieved October 6, 2003, from http://www.theiia.org/download.cfm?file=22398.

Houck, T. P. (2003). *Why and How Audits Must Change*. New Jersey: USA, John Wiley & Sons, Inc.

Humphrey, J., & Schmitz, H., (1998). Trust and Inter Firm Relations in Developing and Transition Economies. *Journal of Development Studies,* 34(4), 33-61.

Hunton, J. E., Bryant, S. M., & Bagranoff, N. A. (2004). *Core Concepts of Information Technology Auditing.* USA: John Wiley & Sons, Inc.

IASB & FASB. (2006, May 16th) Conceptual Framework – Joint Project of the IASB and FASB. Retrieved June 9th, 2006, from http://www.fasb.org/project/conceptual_framework.shtml.

IIA Adviser. (2006). *Audit Committee Survey*. I A Adviser, Institute of Internal Auditors South Africa. February, 15-17.

Iluka Resources Limited. (2005, March). Audit and Risk Committee Charter. Retrieved, 2006, February 16, from http://www.iluka.com/pdf/0503_Audit_Risk_Committee_Charter.pdf

Integrity Incorporated (n.d.) Corporate Governance FAQ - *Due Diligence,* Retrieved October 9, 2005, from http://www.integrityincorporated.com/corporateFAQ.aspx#faq5

Iskander, M., & Chamlou, N. (2000). *Corporate Governance: A Framework for Implementation, (Report no. 20829).* Washington D. C., USA: The World Bank Group.

ISO/IEC 13335-3 Technical Report. (1998). *Information Technology – Guidelines for management of IT Security*. Part 3: Techniques for he management of IT Security. International Standard Organization.

ISO/IEC 17799. (2005). *Information Technology - Security Techniques - Code of practice for information security management.* International Organization for Standards. Web site: http://www.iso.org/iso/en/ISOOnline.frontpage.

IT Control Objectives for Sarbanes-Oxley. (2004). USA: IT Governance Institute.

ITGI. (2003). *IT Governance Executive Summary*. Retrieved May 16, 2004, from http://www.itgi.org

ITGI. (2004). *Managing Enterprise Information Integrity: Security, Control and Audit Issues.* USA: IT Governance Institute.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. In T. Clarke (Ed.) *Theories of Corporate Governance* (pp. 58-63). UK & New York: Routledge

Johnson-George, C., & Swap, W. C. (1982). Measurement of Specific Interpersonal Trust: Construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology*, 43(6), 1306-1317.

Jordan, E. & Silcock, L. (2005). *Beating IT Risks*. England: John Wiley & Sons, Ltd.

Jung, W. (2004). A Review of Research: an Investigation of the Impact of Data Quality on Decision Performance. *ACM International Conference Proceeding Series*, 90, 166-171.

Jurors see tape of Kozlowki's party. (2003, October 29). *CNNMoney*. Retrieved October 6, 2004, from http://money.cnn.com/2003/10/28/news/companies/tyco_party/index.htm?cnn=yes

Kellermann, K., & Reynolds, R. (1990). When Ignorance is Bliss: The role of motivation to reduce uncertainty in uncertainty reduction theory. *Human Communication Research,* 17 (1), 5-75.

Khare, R., & Rifkin, A. (1998). Weaving a Web of Trust. Retrieved March 12, 2005, from http://www.w3j.com/7/s3.rifkin.wrap.html.

Kimbrough, S. O. (2005). Foraging for Trust: Exploring Rationality and the Stag Hunt Game. Retrieved April 12, 2005, from http://opim.wharton.upenn.edu/~sok/sokpapers/2005/itrust-2005-final.pdf.

King II Report, (2002). *King Report on Corporate Governance for South Africa*. South Africa: Institute of Directors in Southern Africa.

Kogan, A., Nelson, K., Srivastava, R., Vasarhelyi, M., & Bovee, M. (1998). Design and Applications of an Intelligent Financial Reporting and Auditing Agent with net Knowledge. Retrieved January 9, 2005, from https://kuscholarworks.ku.edu/dspace/bitstream/1808/141/1/srivastava.pdf.

Kogan, A., Sudit, F., & Vasahelyi, M. (2000). Some Auditing Implications of Internet Technology. Retrieved February 16, 2005, from http://www.rutgers.edu/accounting/raw/miklos/tcon3

Krell, E. (2004). "Continuous" will be key to compliance. *Business Finance Magazine*. Retrieved January 24, 2005 from Website www.businessfinancemag.com, December 2004 release.

Kydd, A. H. (2005). *Trust and Mistrust in International Relations*. Princeton, USA: Princeton University Press.

Larzelere, R.E., & Huston, T.L. (1980). The Dyadic Trust Scale: Toward understanding interpersonal trust in close relationships. *Journal of Marriage and the Family,* 42; 595-604

Law.Com Dictionary (2005a) – *due-care* http://dictionary.law.com/default2.asp?selected=592&bold=%7C%7C%7C%7C

Law.Com Dictionary (2005b) – *substantive law* http://dictionary.law.com/default2.asp?selected=2049&bold=%7C%7C%7C%7C

Leblanc, R., & Gillies, J. (2003). The Coming Revolution in Corporate Governance. *Ivey Business Journal: Improving the Practice of Management*. Retrieved March 11, 2005, from http://www.csae.com/client/csae/CSAEHome.nsf/object/2004+Conference/$file/r-leblanc.pdf

Leeladhar, V. (2005) Basel II Accord and its Implications. Retrieved January 14, 2006, from http://www.bis.org/review/r050321f.pdf

Lev, B. (2001). *Intangibles: Management, Measurement, and Reporting.* Washington, D. C., USA: Brookings Institute Press. Retrieved February 10, 2004, from http://www.icgrowth.com/resources/documents/Brookings-Lev-Intangibles-01.02.20.pdf.

Limerick, D., & Cunnington, B. (1993). *Managing the new organization: A Blueprint for Networks and Strategic Alliances.* San Francisco: Jossey-Bass.

Lindberg, D. (2005). Corporate Governance – The Role of the Audit Committee. To be published in *Risk Management Journal* in fall of 2005. Retrieved the July 9, 2005, from http://www.cob.ilstu.edu/katie/WorkingPapers /CorporateGoverance-Paper1%5B1%5D.isu.doc.

Lowenstein, L. (2003b). *A Perfect Storm: Changing a Culture*. Swedish Corporate Governance Forum Stockholm. Retrieved April 16, 2005, from http://www.law.columbia.edu/center_program/law_economics/wp_listing_1/wp_author?exclusive=filemgr.download&file_id=95189&rtcontentdisposition=filename%3DWP256.pdf

Lowenstein, R. (2003a, October 12). Can corporate America curb the monster? *Wahsingtonpost.com*. Retrieved October 10, 2004, from http://www.washingtonpost. com/ac2/wp-dyn?pagename=article &contentId=A10979-2003Oct&=true

Luhmann, N. (1998). Familiarity, Confidence, Trust: Problems and Alternatives. In D. G. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations.* 94-107. New York: Basil Blackwell.

Lundholm, R. J. (1999). Reporting on the Past: A New Approach to Improving Accounting Today. University of Michigan Business School. Retrieved 16 June 2005 from http://www.sec.gov/rules/proposed/s70300/lundholp.htm

Machlup, F. (1983). Semantic Quirks in Studies of Information. In F. Machlup, U. Mansfield (Eds.). *The Study of Information: Interdisciplinary Messages*. 641-671. New York: John Wiley & Sons.

Machlup, F. & Mansfield, U. (1983). *The Study of Information: Interdisciplinary Messages*. New York: John Wiley & Sons.

Marks, N. (2001). The new age of internal auditing, The Institute of Internal Auditors, Florida, Retrieved October 11, 2004, from http://www.theiia.org/index.cfm?act=home.login&return=doc_id=2738

Marchany, R. (2002). Seven-step IT Risk Assessment. *IT Audit,* 5, Retrieved August 16, 2003, from http://www.theiia.org/iia/index.cfm

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, 20(3), 709-734.

Mellon Financial Corporation. (2006, January). Charter of the Risk Committee of the Board of Directors. Retrieved, 2006, February 16, from http://www.td.com/governance/risk_charter.pdf

Merriam-Webster Online Dictionary. *Corporate Governance*. Retrieved July 11, 2005, from http://m-w.com/cgi-bin/dictionary?book=Dictionary&va=govern

Mesarvic, M. D. (1983). Mathematical Systems Theory and Information Science. In F. Machlup, U. Mansfield (Eds.). *The Study of Information: Interdisciplinary Messages*. 641-671. New York: John Wiley & Sons.

Millstein, I. M. (1999). Introduction to the Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees. *The Business Lawyer*, 54 (3), 1057-1066.

Mishra, A. K. (1996). Organizational Responses To Crisis: The centrality of trust. In R. M. Kramer & T. R. Tyler (Eds.). *Trust in organizations: Frontiers of theory and research*: 261-287. California: Sage.

Mittner, M. (2003, July 28). What happened at Saambou? *Finance24.Com*. Retrieved February 2, 2005, from http://www.finance24.com/articles /companies/display_article.asp?ArticleID=1518-24_1394171

Mittner, M. (2005, September 5). Scorpions Open Can of Worms. *Finance24.Com*. Retrieved September 5, 2005, from http://www.finance24.com/articles/companies/display_article.asp?Nav=ns&lvl2=comp&ArticleID=1518-24_1765266

Morris, B. W. (2002). *Identifying Risks and Building Trust in Global Supply Chains*. Retrieved May 14, 2003, from Columbia/Wharton Center for Risk Management and Decision Processes on, Risk Management Strategies in an Uncertain World http://www.ldeo.columbia.edu/res/pi/CHRR/Roundtable/Notes.html.

Morrison, A. D. (2004, July 22) *Sarbanes-Oxley, corporate governance and operational risk.* In: Proceedings of the Sarbanes-Oxford Conference held at Said Business School, University of Oxford.

Mouton, J. (2001). *How to succeed in your Master's and Doctoral Studies: A South African Guide and Resource Book*. Pretoria: Van Schaik Publishers.

Murphy, P. (1991). Game Theory Models for Organizational/Public Conflict. *Canadian Journal of Communication*, 16(2). Retrieved March 9, 2005, from http://info.wlu.ca/~wwwpress/jrls/cjc/BackIssues/16.2/murphy.html.

Myers, M. D. (1997). Qualitative Research in Information Systems. *MISQ Discovery*, June. Webdsite: http://www.qual.auckland.ac.za/

NACD. (1999, October 6th). *Blue Ribbon Commission on Audit Committees*. National Association of Corporate Directors, Washington, DC:USA.

NACD. (2004). *Audit Committees: A Practical Guide: A report of the NACD Blue Ribbon Commission*. National Association of Corporate Directors, Washington, DC: USA.

Necessary and Sufficient Conditions. (2006). Stanford Encyclopaedia of Philosophy. Retrieved October 16, 2006, from *http://plato.stanford.edu/entries/necessary-sufficient/*

Nisenzoun, F. (2004). *The Correlation of Executive Compensation and Shareholder Wealth*. Stanford University. Retrieved July 22, 2005, from http://wwwecon.stanford.edu/academics/Honors_Theses/Theses_2003/Nisenzoun.pdf

NIST 800-53 Publication. (2005). *Information Security*. National Institute of Standards and Technology. US Department of Commerce. Web site: http://www.csrc.nist.gov/publications/nistpubs/index.html.

NIST 800-12 Handbook. (1995). *An Introduction to Computer Security.* National Institute of Standards and Technology. US Department of Commerce. Web site: http://www.csrc.nist.gov/publications/nistpubs/index.html.

Noorderhaven, N. G. (1996). Opportunism and Trust in Transaction Cost Economies. In J. Groenewegen (Ed.), *Transaction Cost Economics and Beyond.* 105-128. Boston: Kluwer Academic.

Oates, B. J. (2006) Researching Information Systems and Computing. London, UK: Sage Publications Ltd.

O'Brien, J. A. (2000) *Introduction to Information Systems: Essentials for the Internetworked Enterprise* (9th Ed.).USA: McGraw-Hill Companies, Inc.

OECD. (2004). *OECD Principles of Corporate Governance*. Organisation For Economic Co-Operation and Development. France: OECD Publication Service.

Olivier, M. S. (2004). *Information Technology Research: A Practical Guide for Computer Science and Informatics* (2nd Ed.). Pretoria: Van Schaik Publishers.

Ong, C. H., & Lee, H. S. (2000). Board functions and firm performance: A review and directions for future research. *Journal of Comparative International Management,* 3 (1). Retrieved February 2, 2005, from http://www.lib.unb.ca/Texts/JCIM/bin/get.cgi?directory=vol3_1/&filename=haut.htm

Onions, R. L. (2003). *Towards a paradigm for continuous auditing*. Retrieved August 20, 2004, from University of Salford, Web site: http://www.continuousauditing.org/index.htm, 2003.

Oud, E. J. (2005). The Value to IT of Using International Standards. *Information Systems Control Journal*, 3.

Oz, E. (2002) *Management Information Systems* (3rd Ed.). Canada: Course Technology Thomson Learning.

Parmalat sues banks for Euro4.4 bn. (2005, August 7). *Finance24.com*. Retrieved August 7, 2005, from http://www.finance24.com/articles/default/display_article.asp?Nav=ns&ArticleID=1518-1783_1750431

Partington, A. (Ed.). (1996). *The Oxford Dictionary of Quotations* (4th Ed.). Oxford New York: Oxford University Press.

Pearce, W. B. (1974). Trust in interpersonal communication. *Speech Monographs*, 41(3), 236-244.

Peltier, T. R. (2001). *Information Security Risk Analysis*. USA: CRC Press LLC.

Phillips, K. (2003). How Wealth Defines Power. *The American Prospect*, 14 (5). Retrieved July 9, 2005, from http://www.prospect.org/print/V14/5/phillips-k.html

Piper, R. (2002). Restoring Trust in Corporate Practices. *Harvard Management Update.* Retrieved June 4, 2003, from Harvard Business Online database.

Pitt, H. L. (2002). Testimony Concerning the Corporate and Auditing Accountability, Responsibility, and Transparence Act. U.S. Securities & Exchange Commission. Retrieved 16 June 2005 from http://www.sec.gov/news/testimony/032002tshlp.htm

QltInc. (2006, January). Audit and Risk Charter. Retrieved, 2006, February 16, from http://www.qltinc.com/Qltinc/main/mainpages.cfm?InternetPageID=209

Quinion, M. (2005). *World Wide Words*. Retrieved July 11, 2005, from http://www.worldwidewords.org/qa/qa-gub1.htm

Ratnasingham, P., & Kumar, K. (2000). Trading Partner Trust in Electronic Commerce Participation. *International Conference on Information Systems, Proceedings of the twenty first international conference on Information systems.* Australia. Retrieved February 12, 2005, from http://delivery.acm.org/10.1145/360000/359811/p544-ratnasingham.pdf?key1=359811&key2=8961420311&coll=GUIDE&dl=GUIDE&CFID=56450121&CFTOKEN=36588837

Reagan, R. (1996) Columbia World of Quotations. Retrieved October 2, 2004, from http://www.bartleby.com/66/86/46086.html

Rechtman, Y. (2004). Continuous Auditing and XBRL, the Trusted Professional. NYSSCPA, 7 (8), Retrieved January 11, 2005, from http://www.nysscpa.org/trustedprof/504/tp13.htm

Rector, N. & Davis, K. (2005) CEO/CFO Certification for Crown Corporations. Retrieved December 12, 2005, from http://www.deloitte.com/dtt/article /0,1002,sid%253D68725%2526cid%253D95172,00.html

Redman, T. C. (1998). The Impact of Poor Data Quality on the Typical Enterprise. *Communications of the ACM*, 41(2), 79-82.

Rezaee, Z., Elam, R., & Sharbatoghlie, A. (2001). Continuous Auditing: the Audit of the Future. *Managerial Auditing Journal*, 13(3), 732-736.

Rezaee, Z., Shabatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. *Auditing: A Journal of Practice and Theory*, 21 (1), 147-163.

Rich, L. (2006, January 13) Sarbanes-Oxley Draws Renewed Criticism. Retrieved February 2, 2006, from http://www.inc.com/criticalnews/articles/200501/sarbox.html

Ring, P. S., & Van De Ven, A. H. (1992). Structuring Cooperative Relationships Between Organizations. *Strategic Management Journal,* 13, 483–498.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*, 23(3), 391-404.

Russell, S. & Norvig, P. (2003) *Artificial Intelligence: a Modern Approach*. (2nd Ed.). New Jersey, USA: Prentice Hall.

Saambou execs in court. (2005, September 14). *Finance24.com*. Retrieved September 15, 2005, from http://www.finance24.com/articles/default/display_article.asp?Nav=ns&ArticleID=1518-24_1770401

Sarbanes-Oxley Act. (2002, July 30). United States of America 107th Congress. Retrieved January 19, 2004, Web site: http://www.sec.gov/about/laws/soa2002.pdf

SAS. (2006) Free Business Intelligence Special Report. Retrieved July 7, 2006, from http://www.sas.com/ads/bireport_google.index.html

Shannon, C. E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*. Retrieved November 11, 2005, from http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html

Shannon, C. E., & Weaver, W. (1949). *The Mathematical Theory of Communication*. Urbana IL, USA: University of Illinois Press.

Shaw, J. C. (2003). *Corporate Governance & Risk: A Systems Approach*. New Jersey: John Wiley & Sons, Inc.

Sinclair, D. (2005). Introduction to Assurance. Retrieved April 9, 2005, from http://www.computing.dcu.ie/~davids/courses/CA548/Introduction_to_Assurance.pdf.

Smith, A. (1981). *An Inquiry into the Nature and Causes of the Wealth of Nations*. R. H. Campbell, A. S. Skinner, & W. B. Todd (Eds.). Indianapolis: Liberty Fund, Inc.

Smith, G. (2005). Disney as a Call to Arms for Shareholders. *Conglomerate*. Retrieved August 22, 2005, from http://www.theconglomerate.org/2005/08/disney_as_a_cal.html

Smith, H., & Fingar, P. (2003). *Business Process Management: The Third Wave*. Florida: Meghan-Kiffer Press.

Solomon, D. (2005, October 17) Critics say Sarbanes-Oxley's costs are too high. *The Wall Street Journal*. Retrieved December 6, 2005, from http://www.post-gazette.com/pg/pp/05290/590143.stm

Sorkin, A. R. (2006, January 29) Public Companies, Singing the Blues. New York Times: Money and Business/Financial Desk pg.4. Retrieved February 3, 2006, from http://www.nytimes.com/2006/01/29/business/yourmoney/29deal.html?ex=1139634000&en=5aea949837ffceb1&ei=5070

Spafford, G. (2004). Control Framework Misconceptions. *IT Management: Network & Systems Management*. Retrieved July 12, 2005, from http://itmanagement.earthweb.com/netsys/article.php/3439901.

Spatt, C. S. (2005, June 9). *Speech by SEC Staff: Governance, the Board and Compensation*. Retrieved August 21, 2005, from http://www.sec.gov/news/speech/spch060905css.htm

Spielberg, N., & Anderson, B. D. (1987). *Seven Ideas That Shook the Universe*. Canada: John Wiley & Sons, Inc.

Spira, L. F. (2003). Audit Committees: begging the question? *Corporate Governance: An International Review*, 11 (3), 180.

Srinivas, S. (2006). *Continuous Auditing Through Leveraging Technology*. Retrieved May 1, 2006, from website www.isaca.org

Stair, R. & Reynolds, G. (2006) Principles of Information Systems. (7th Ed.). Massachusetts: USA, Thomson Course Technology.

Sullivan, M. F. (2000). *Flunking The Duty Of Care, The Four Most Common Mistakes Made By Directors*. Retrieved June 1, 2005, from http://www.bricker.com/Publications/articles/157.asp.

Sunnafrank, M. (1986). Predicted Outcome Value During Initial Interactions: A Reformulation of Uncertainty Reduction Theory. *Human Communication Research*, 13 (1), 3-33.

Taylor, P. (2005, January). The perils of systems-based fraud. *IT Audit, 8*.

Texas A&M University (2005) The Center for Continuous Auditing. Available from Web site: http://raw.rutgers.edu/continuousauditing/

Tricker, R. I. (1994). *International Corporate Governance*. Singapore: Prentice-Hall.

Todd, A. (2005). *The Challenge of Online Trust: For online and offline business*. Retrieved July 15, 2005, from website http://www.trustenablement.com/trust_enablement.htm#RiskManagement

Toronto-Dominion Bank. (2005, November). Risk Committee of the Board of Directors: Charter – Supervising the Management of Risk of the Bank. Retrieved, 2006, February 16, from http://www.td.com/governance/risk_charter.pdf

Tully, S. (2003, September 15). Dick Grasso: See Dick Squirm. *Fortune*. Retrieved October 19, 2004, from http://bear.cba.ufl.edu/demiroglu/fin4504fall2004/Articles/Article09.htm

Tuomi, I. (1999). Data is More Than Knowledge: Implications of the Reversed Knowledge Hierarchy for Knowledge Management and Organisational Memory. *Journal of Management Information Systems*, 16(3), 1003-117.

Turnbull Report. (1999). *Internal Control: Guidance for Directors on the Combined Code.* UK: The Institute of Chartered Accountants in England & Wales.

U.S.A. Senate. (2002). *The role of the board of directors in Enron's collapse*. Permanent Subcommittee on Investigations of the Committee on Governmental Affairs. United States of America 107th Congress, 2nd session. Retrieved November 22, 2004, Web site: http://hsgac.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=451&Affiliation=C

Vasarhelyi, M. A. (2002). Concepts of Continuous Assurance. Retrieved February 16, 2004, from Web site: http://raw.rutgers.edu/continuousauditing/

Vasarhelyi, M. A., & Halper, F. B. (1991). The Continuous Audit of Online Systems. *Auditing: A Journal of Practice and Theory, 10*(1).

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2003). Principles of analytic monitoring for continuous assurance, in: *Proceedings of the Fifth Continuous Auditing Symposium held at Rutgers Business School*, Web site: http://raw.rutgers.edu/continuousauditing/

Von Bertalanffy, L. (1968). *General Systems Theory*. Middlesex, England: Penguin Books Ltd.

Von Neumann, J., & Morgenstern, O. (1964). *Theory of Games and Economic Behaviour.* New York, USA: Science Editions, John Wiley & Sons

Von Solms, S. H. (2003). IT Governance & Information Technology Risks (Module 7). *In Governance, Risk & Ethics.* In Association With The Institute of Directors, RAU & E-Degree. Johannesburg: South Africa.

Walker, J. (2003). *The 2000-03 Nasdaq Bear Market vs. 1929 Crash*. Retrieved September 2, 5005, from http://www.lowrisk.com/nasdaq-1929.htm.

Walsh, J. P., & Seward, J. K. (1990). On the Efficiency of Internal and External Corporate Control Mechanisms. *The Academy of Management Review*, 15 (3), 421-458.

Wand, Y., & Wang, R. Y. (1996). Anchoring Data Quality Dimensions in Ontological Foundations. *Communication of the ACM*, 39(11), 86-95.

Wang, R. Y., & Strong, D. M. (1996). Beyond Accuracy, What Data Quality Means to Data Consumers. *Journal of Management Information Systems*, 12(4), 5-34.

Ward, J., & Peppard, J. (2002). *Strategic Planning for Information Systems.* England: John Wiley & Sons Ltd.

Ware, L. C. (2002). CSO Research Reports: Security Spending – How much is enough?. Retrieved October 9, 2005, from http://www.csoonline.com/csoresearch/report6.html

Warren, J. D., & Parker, X. L. (2003). *Continuous Auditing: Potential for Internal Auditors*. Florida: The Institute of Internal Auditors.

Wessmiller, R. (2002). *Facing the Data Integrity Challenge*. Retrieved 20 April, 2005, from http://www.theiia.org/itaudit/index.cfm?fuseaction=print&fid=440

Westby, J. R. (2004). *Information Security: Responsibilities of Boards of Directors and Senior Management.* Retrieved May 29, 2005, from http://www.reform.house.gov/UploadedFiles/Westby1.pdf.

Westlake, M. (2003) Delay to final Basel II accord "inevitable". Global Risk Regulator. Retrieved December 6, 2005, from http://www.globalriskregulator.com/archive/JulyAugust2003-02.html

Westphal, J. D., & Zajac, E. J. (1998). The Symbolic Management of Stockholders: Corporate Governance Reforms and Shareholder Reactions. *Administrative Science Quarterly*, 43, 127-153.

Whitman, M. E., & Mattord, H. J. (2003). Principles of Information Security. USA: Thomson Course Technology.

Wilson, B. (Ed.). (2002). *Internal Controls Assurance: A guide to board level reporting*. UK: National Housing Federation.

Woodroof, J., & Searcy, D. (2001). *Continuous Audit: Model Development and Implementation within a Debt Covenant Compliance Domain*. Retrieved October 14, 2004, from Rutgers Business School, Web site: http://raw.rutgers.edu/continuousauditing/.

Woods, J. *Work in Progress*. Whole Systems Quotes. Retrieved February 20, 2004, from http://www.worldtrans.org/whole/wsquotes.html

Zacharias, C. (2000). Corporate Governance: The Audit Committee on the Firing Line - New Rules, New Responsibilities. Retrieved, May 14, 2005, from http://www.aicpa.org/pubs/jofa/aug2000/zachar.htm.

Zald, M. N. (1969). The power and functions of boards of directors: A theoretical synthesis. *American Journal of Sociology*, 74, 97-111.

Zajac, E. J., & Westphal, J. (1994). The costs and benefits of managerial incentives and monitoring in large U.S. corporations: When is more not better? *Strategic Management Journal,* 15, 121-142.

Zand, D. E. (1972). Trust and Managerial Problem Solving. *Administrative Science Quarterly*, 17(2), 229-239.

Zuccato, A. (2005). Holistic Information Security Management Framework for electronic commerce. Karlstad, Sweden: Karlstad University Press.

APPENDICES

The following papers were presented and published whilst conducting research towards this thesis.

A:

Flowerday, S., & Von Solms, R. (2006). Trust: an Element of Information Security. Presented at IFIP/SEC 2006, Karlstad, Sweden. Published in S. Fischer-Hubner, K. Rannenberg, L. Yngstrom, S. Lindskog (Eds.). Security and Privacy in Dynamic Environments. 87-98. IFIP. USA: Springer.

B:

Flowerday, S., & Von Solms, R. (2005a). Real-time Information Integrity = System Integrity + Data Integrity + Continuous Assurances. *Computers & Security*, 24(8), 604-613.

C:

Flowerday, S., & Von Solms, R. (2005b). Continuous Auditing: Verifying Information Integrity and Providing Assurances for Financial Reports. *Computer Fraud & Security*, 7, 12-16.

D:

Flowerday, S., Blundell, A., & Von Solms, R. (2006). Continuous Auditing Technologies and Models: A discussion. *Computers & Security, 25*(5), 325-331.

Trust: an Element of Information Security

Stephen Flowerday and Rossouw von Solms

The Centre for Information Security Studies, P. O. Box 77000, Nelson Mandela Metropolitan University, Port Elizabeth, 6031, South Africa
sflowerday@telkomsa.net; rossouw.vonsolms@nmmu.ac.za

Abstract. Information security is no longer restricted to technical issues but incorporates all facets of securing systems that produce the company's information. Some of the most important information systems are those that produce the financial data and information. Besides securing the technical aspects of these systems, one needs to consider the human aspects of those that may 'corrupt' this information for personal gain. Opportunistic behaviour has added to the recent corporate scandals such as Enron, WorldCom, and Parmalat. However, trust and controls help curtail opportunistic behaviour, therefore, confidence in information security management can be achieved. Trust and security-based mechanisms are classified as safeguard protective measures and together allow the stakeholders to have confidence in the company's published financial statements. This paper discusses the concept of trust and predictability as an element of information security and of restoring stakeholder confidence. It also argues that assurances build trust and that controls safeguard trust.

1. Introduction

Trust and controls help curtail opportunistic behaviour, therefore confidence in information security management can be achieved. Besides the technical aspect of information security and IT that should be implemented using best practices, one needs trust to help curb 'cheating' and dishonesty. This paper focuses on the information found within the financial statements of a company. Stakeholder, especially investor, confidence needs to be restored in the board of directors in the domain of financial reporting. The avalanche of corporate governance scandals such as Enron, WorldCom, Tyco, and Parmalat has caused many to be suspicious of the information found within financial statements.

It has been necessary to draw from the work in other research disciplines to extend the study of trust and risk to this domain. This fragile, yet important concept, *trust*, greases the wheels of industry. Trust allows the various users of information, found within information systems, confidence when making decisions.

An important aspect of corporate governance is the management of risk. Companies today use a system of controls in their efforts to manage their risk. Often these controls focus on the company's various financial processes and systems. The reason for this is that these important processes and systems are often the target of

security breaches. It has therefore become imperative that the security for these systems is comprehensive. Both opportunistic behaviour, which involves a human element, and the conventional technical IT security threats, need to be addressed.

It is stressed that [1], *"security is not a separable element of trust"*. This statement collaborates that both trust and security-based mechanisms are classified as safeguard protective measures [2]. Together these provide technological, organisational and relationship benefits to the various company stakeholders.

This paper introduces the concept of trust and uncertainty reduction followed by what constitutes trustworthiness. Self-centred opportunism, 'cheating' and dishonesty are classified as unfavourable behaviour, consequently behaviour is addressed using game theory to illustrate possible outcomes. The very close relationship that trust and risk have, is discussed with assurances being emphasised as an element to help build trust. Finally, a trust strategy is emphasised as a way to avoid unfavourable behaviour and to build and safeguard the concept of trust.

2. The Theory of Trust

Trust should not be left in the domain of philosophers, sociologists, and psychologist but also needs to be addressed by all attempting good governance. Can there be any doubt that fairness, accountability, responsibility, and transparency [3] are facets that contribute to the building and safeguarding of trust? Trust is not something that simply happens. It is fragile and not easily measured or identified [4].

2.1 Uncertainty Reduction Theory and Trust

In general, trust is defined as a psychological state comprising the intention to accept vulnerability, based upon positive expectations of the intentions or behaviour of another [5]. Trust also refers to the notion of the degree one risks: this risk is predicated on the belief that the other party is beneficent and dependable [6]. The notion of trust is that it involves the willingness of a trustee [7] *(the recipient of trust or the party to be trusted, i.e. board of directors)* who will perform a particular action important to the trustor *(the party that trusts the target party or the trusting party, i.e. investors)*.

If no uncertainty exists between the two parties, it indicates that no risk or threat is found in future interaction between the parties [8]. Noting that we do not live in a perfect world and we don't have perfect competition it is therefore impossible to have absolute uncertainty free interaction *(in other words, a degree of uncertainty always exists)*. One needs to make an effort to reduce uncertainty and to increase predictability about how the other party will act. Both the board of directors and the various company stakeholders should consider this.

It is emphasised that through communication and the exchange of information about each party, a decrease in uncertainty occurs [9]. According to Berger [10] uncertainty about the other party is the *"(in)ability to predict and explain actions"*. Thus the basic premise of Uncertainty Reduction Theory, if one applies the principles to the various company stakeholders, is that it attempts to reduce uncertainty and to

increase predictability about each party's behaviour. This confirms that uncertainty can only be reduced by the information shared and a knowledge as to the condition of this information, which will affect the (un)certainty level [10].

Without a certain degree of predictability, a party has no basic assumption of how the other party will or will not utilise their trusting behaviour [8]. When one party is able to predict a degree of the other party's future actions this leads to a decrease in one's perceived vulnerability *(risk is perceived to be reduced)*. Therefore uncertainty reduction is a necessary condition for the development of trust. One's predictability about the other should be increased, thus reducing uncertainty via communicating (producing financial statements for the various stakeholders) with the other party. As a result: when more uncertainty is reduced, perceived predictability should be increased and vulnerability will be minimised (based upon prior experience). This highlights the paramount importance that the information found within the company financial statements has its integrity intact. If not, a trust problem will occur.

2.2 Trustworthiness

Fig. 1 is a proposed model of trust of one party for another which highlights the elements of trustworthiness [7]. This model illustrates that the level of trust and the level of perceived risk in a situation will lead to risk-taking in a relationship. It also touches on a trustor's propensity, which is said to be influenced by how much trust one has for a trustee prior to information on that particular party being available. Propensity will differ in a party's inherent willingness to trust others [7].

In this model, the three elements that help to create and define a trustworthy party are discussed. These elements are: *Integrity, Benevolence,* and *Ability*. This perception of trust can be applied to corporate governance in the following way:

- Integrity-based trust refers to whether the directors are honest and fair and not '*fudging the numbers'*. Some scholars in their research have used the words *reliability* or *predictability* in place of integrity [2, 11].
- Benevolence-based trust implies that the directors would be loyal, keep the best interests of the various company stakeholders at heart, and not seek to be self-serving and opportunistic. Some scholars have used the words *goodwill* or *openness* in place of benevolence [2, 11].
- Ability-based trust relates to the director's *skill level,* for example, their technical competence and understanding of information systems and security. Some researchers favour the word *competence* rather than *ability*, however, little difference is found in the meanings of these words [2, 11, 12].

Perceived trustworthiness requires honesty and integrity. These are attributes that a party needs to demonstrate so that when opportunities to *'cheat'* arise, they will be turned down. As stated [7], *"… if the trustee had something to gain by lying, he or she would be seen as less trustworthy"*. In addition, the more perceived benevolence and integrity found in a party, the more likely it will be to predict a favourable future outcome for a relationship with that party [13].

Appendix A

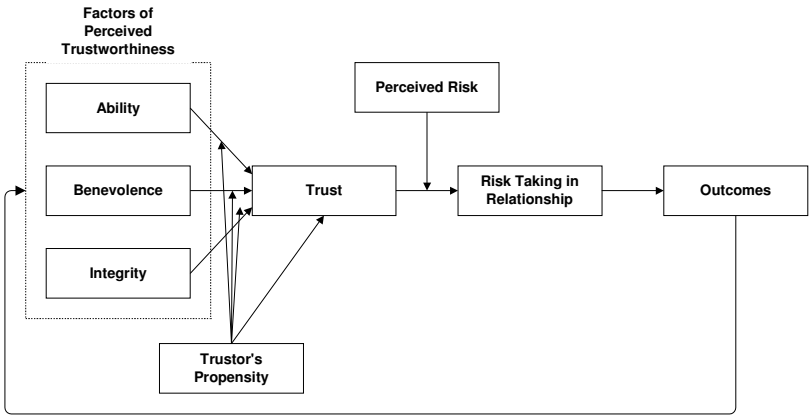

Fig. 1. Proposed Model of Trust [7].

2.3 Trust, Behaviour and Game Theory

Perceived risk and trust affect behaviour and this varies at different stages of a relationship [14]. Risk is dominant in the early stages and trust, in long-term relationships. One needs to consider the *cause and effect* relationship between *trust and risk,* which have an effect on *behaviour.* This view of trust is important because in order to build trust, the perceived risks by the various company stakeholders, especially investors, need to be catered for to avoid unfavourable behaviour.

Gefen et al. [14], from their research, found that the risk perception is more than a mere "*moderating influence"* affecting behaviour. They claim that the perceived risk "*mediates"* the affect trust has on behaviour. This, again, highlights the importance of information security in reducing the *'threats'* (both human and technical) that financial information systems are exposed to.

Economists and mathematicians have used game theory in their study of trust since 1944 [15]. These formal trust models consider how *'players'* discover trust and can quantify how trust or mistrust can occur [16, 17]. This paper discusses the principles of two games and the mathematical route will not be pursued.

Game theory involves the behaviour of rational decision makers *(players)*, whose decisions affect each other. These players could be the company investors and managers, or any of the company stakeholders that may have conflicting interests. As emphasised [17, 18], an essential element of game theory involves the amount of information known about each other by the various players. The information the various players have will determine their behaviour. Also to be noted are the *'rules'* of the game (codes, regulations, policies, etc. that the company needs to comply to).

A classic example of game theory is known as the Prisoner's Dilemma. There are two prisoners in separate cells, faced with the dilemma of whether or not to be police informants. Without further communication, the two players need to trust each other to have integrity and to be benevolent. The following are possible outcomes.

Appendix A

If neither become informants and defect, the police have insufficient or only circumstantial evidence to convict them and therefore both players receive light sentences. If trust is lacking and both turn and become informants for the police, through their defection, both players receive heavy sentences. If one player defects and becomes a police informant, that player is set free and the player that did not defect is convicted and receives a very heavy sentence due to the testimony of the player that defected. The dilemma of the scenario highlights the issue of trusting the other player without continuous communication. Applied to a corporate governance setting the 'communication' could be affected by both the *accuracy* (fraud) and *reliability* (confidentiality, integrity and availability) of the information found within the company financial statements.

As observed [19], if the police were to tell the prisoners (players) that the interrogation is ongoing and without a foreseeable end, a pattern emerges and cooperation can become stable. This is the discovery of trust as the players learn to trust each other over time and the perceived risk element is reduced. If one applies this model of trust to corporate governance it can be assumed that, over time, trust will be established between the various stakeholders, including the CEO, the board of directors and investors.

Axelrod [20] suggests that, with time, a pattern of cooperative behaviour develops trust as in game theory. However, one could trust the director's ability (technical and information security capabilities) but not the integrity of the person behind the systems that may act opportunistically. This highlights that trust is more specific than '*I trust the board of directors'*. One should clarify what it is that I trust the board of directors to do.

To explain this concept another way an everyday example will be used. Note that trust is not transitive and is rather domain specific [21]. Example: one might entrust their colleague with $100 loan, but not entrust the same resource to that colleague's friend whom you do not know. Trust therefore weakens as it goes through intermediaries. Furthermore, to re-emphasise a related aspect, one might trust their colleague by loaning them $100 but not allow them access to your bank account to withdraw the $100 themselves. The second example highlights the domain specificity of trust. One does not blindly trust, but one trusts a party in a specific area or domain.

To continue with the prisoner's dilemma, the interests of the players are generally in conflict. If one chooses the high-risk option and the other chooses the low, the former receives a maximised positive outcome and the latter a maximised negative outcome. There are cases of opportunistic behaviour, such as the directors of the over-valued telecommunications companies who cashed in and sold their shares totalling more than US$6 billion in the year 2000, yet they touted the sector's growth potential just as it was about to collapse [22]. The investors chose the high risk option and remained committed while many directors 'defected' choosing the low risk option and short term financial gains.

Kydd [23] stresses a different point of the Prisoner's Dilemma by pointing out that, strictly speaking, there is no uncertainty about motivations, or behaviour and the dominant strategy would be to defect. As a result, uncertainty is smuggled in through the back door. He emphasises that *"…trust is fundamentally concerned with this kind of uncertainty"*. Kydd's research discusses trust and mistrust, and, claims that there is no uncertainty in the prisoner's dilemma about whether the other side prefers to

sustain the relationship. He questions whether future payoffs are valued highly enough to make sustained cooperation worthwhile, or whether they are not and the parties will defect. He states that trust is therefore perfect or nonexistent. To model trust in the prisoner's dilemma one must introduce some uncertainty, either about preferences or about how much the parties value future interactions [23]. Applying Kydd's argument to the various company stakeholders illustrates that there needs to be a *win win* situation for all. The information one party has, needs to be had by the other parties as well. Conflicts of interest need to be avoided so that the benefits of opportunistic behaviour are minimised.

Another game theory game, the *Stag Hunt*, is less well known than the Prisoner's Dilemma, however, its probably more suited to this paper. Moreover, the Stag Hunt game is also known as the *Assurance Game.* Assurance being core to building trust highlights the importance of this game. An important focus is, if one-side thinks the other will cooperate, they also prefer to cooperate. This means that players with the Assurance Game preferences are trustworthy. Kydd states: *"They prefer to reciprocate cooperation rather than exploit it"*. This denotes that it makes sense to reciprocate whatever one expects the other side to do, trust or suspicion.

The Stag Hunt (assurance game) is about two hunters who can either jointly hunt a stag (an adult deer/buck, a rather large meal) or individually hunt a rabbit (tasty, but substantially less filling). Hunting a stag is quite challenging and requires mutual cooperation. If either hunts a stag alone, the chance of success is minimal. Hunting a stag is most beneficial for the group however, requires a great deal of trust among its members. Each player benefits most if both hunt stag. Thus, hunting a stag both players trust their counter-player to do the same. Conversely, a player hunting rabbit lacks trust in the counter-player. Deciding not to risk the worst possible outcome (not getting the stag) is to decide not to trust the other player. On the other hand, *"if trust exists then risk can be taken"* [16].

Cooperation is possible between trustworthy parties who know each other to be trustworthy. This can be likened to the CEO, the board of directors, and the investors. They need independent and objective assurances that the other party is trustworthy. In the Prisoner's Dilemma, cooperation can be sustainable only if the players care enough about future payoffs because they will fear that attempts to exploit the other party will be met with retaliation [24]. In the Assurance Game (Stag Hunt) the level of trust one party has for the other party is the probability that it assesses the other party as trustworthy [23].

Kydd adds that the minimum trust threshold will depend on the party's own tolerance for the risk of exploitation by the other side. To consider the situation of the CEO, board of directors and the investors, cooperation needs to be the overwhelming option to avoid cheating and mistrust. This leads back to the elements of the trustworthiness model proposed by Mayer et al. [7] that integrity, benevolence and ability are required. The best option is clearly the hunting of the stag together, as it maximises the return on effort and becomes a win win situation. Applied to a corporate setting it illustrates the need for positive cooperation and trust between the various stakeholders and the avoidance of conflicts of interest.

The development of positive uncertainty reduction should be the basis for engaging in cooperative behaviour. When a positive piece of information about the company is presented (financial statements with assurances), the uncertainty will be reduced, as a

result, the chance of engaging in cooperative behaviour will be increased. In contrast, where higher uncertainty levels exist between parties, or a piece of information negatively confirms predictions, then the competitive course of action will more likely to be engaged. In a cooperative situation, both participants feel that they are perceived as benevolent. Therefore they can willingly place themselves in vulnerable positions. Under this condition, the various parties are likely to establish or perceive a relationship of mutual trust. This again highlights the point that the stakeholders need assurances to trust the information found within the financial statements (validation by auditors). This emphasises the importance of information security and that it should safeguard the *accuracy* (fraud) and *reliability* (confidentiality, integrity and availability) of information.

3. Risk, Security and Assurances

It is vital that positive predictability needs to occur for trust to increase between the various parties (stakeholders). Therefore one should ensure that through various security mechanisms, the information found within the financial statements is correct. The knowledge, via independent and objective assurances, that information security is adequate and the risks contained assist in building confidence.

3.1 The Dark-Side of Trust: Risk

Queen Elizabeth 1st in her address to Parliament in 1586 concluded with: *"In trust I have found treason"* [25]. At what stage of a relationship is one relying on trust to the point that one is overly exposed to risk? In perfect competition, Humphrey and Schmitz [26] contend, *"risk is ruled out by the assumptions of perfect information and candid rationality"*. However, they emphasise that in today's world the issue of trust exists because transactions involve risk, as we do not have perfect competition.

Noorderhaven [27] observes that in context of a transaction relationship, if adequate security safeguards are in place for a transaction to go ahead, then it is not a trust transaction. However, if the actual information security safeguards and controls in place are less than adequate, a trust-based relationship is assumed as the existence of trust is inferred.

To expand on this, risk is present in a situation where the possible damage may be greater than the possible return [28]. Therefore, as stated [5], *"risk creates opportunity for trust"*. This is in harmony with Gefen et al. [14] and game theory [18, 20] that postulate that trust can *grow* and *evolve* over time.

It highlights the premise that trust can decrease uncertainty about the future and is a requirement for continuing relationships where parties have opportunities to act opportunistically [29]. This is in agreement with the theory that trust affects the trustor's risk taking behaviour [7]. To summarise, if the level of trust surpasses the perceived risk, one would engage in the relationship. Nevertheless be cautious, as trust is the positive view of risk exposure as *"trust is risk*" [30].

Appendix A

3.2 Trust and Security

Camp [1] is an advocate that both *"technical competence"* and *"good intent"* are required to ensure security. She further emphasises that: efforts at securing systems should involve not only attention to networks, protocols, machines and policies, but also a thorough understanding of how social agents (individuals and parties) participate in, and contribute to trust. One can lose sight of the fact that conventional security technology, if implemented perfectly, still does not equate to trust [19].

Although it may be desirable, 100% security is not feasible and it is commonly accepted that not all risk can be eliminated [31]. This residual or inherent control risk is based on the notion that additional investments in controls or safeguards will not eliminate this type of risk. This means that the various company stakeholders are forced into a trust-based relationship.

It is widely accepted that reduced risk and increased trust are both likely to increase the likelihood of engaging in transactions [14]. DeMaio [32] champions that one should try to build business environments based on each party's willingness and ability to continuously demonstrate to the other's satisfaction that all dealings are honest, open, and that the 'rules' are followed. DeMaio states, *"e-Trust is all about mutual assurance."*

3.3 Mutual Assurance and Confidence

Mutual assurances help to build confidence between the various company stakeholders in a similar manner as with the hunters in the Stag Hunt/Assurance game. In the same manner, VeriSign can provide confidence that an active key-holder has signed a document and it can be assumed that the document is untainted because of VeriSign's independence. Therefore, it follows that auditors verify a company's financial statements (validation) and provide assurances. The only difference is that VeriSign and the Stag Hunt game provides the assurance in real-time, something the auditing profession needs to address.

Mutual assurance should exist between stakeholders, reassuring each other that the risks are mitigated to an acceptable level and that the degree of (un)certainty is appropriate. The adage of *"trust but verify"* should exist as the various stakeholders demonstrate to each other, via objective and independent audits, that the agreed upon best practices are maintained.

The confidence that the various company stakeholders have in their relationship is determined by two factors: one being the level of trust and the other the perception of how adequate or inadequate the controls are that govern the conditions of the arrangement [33]. To achieve a favourable relationship between the stakeholders, one has to find the right *balance* between trust and control.

Fig. 2 illustrates how trust and controls work together in securing a transaction or a business process. Triangle A, B, D is the *Control* area and triangle A, D, C is the *Trust* area. The line E, F is a hypothetical positioning of the company's Risk Appetite. The area of the rectangle A, B, D, C is the business process area or transaction area. When one views the Risk Appetite line (E to F) one will note that the white area is protected by controls and the dark area is the 'risk' exposure or the area protected by

trust. Depending on how much the parties '*trust*' each other will affect the positioning of the Risk Appetite line.

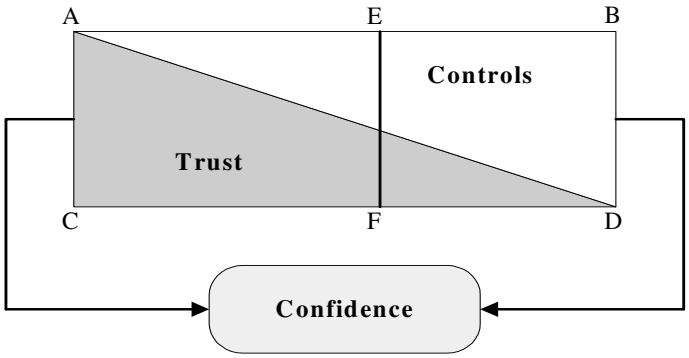

Fig. 2. The Relationship between Trust, Controls and Confidence.

However, to summarise: absolute trust and absolute control are two opposing extremities of approach for attaining confidence (personal communication, Todd, August 2005). The solution is somewhere in the middle ground between trust and control. There are those that argue the company should position itself on the trust side in an effort to reduce costs [34, 35]. However, practicalities and realism are *forces* that pull the solutions into the control end of the spectrum.

4. A Trust Strategy

Strategy, by its nature, concerns itself with the future. Companies today operate in an uncertain world where the markets have become increasingly more competitive. The Turnbull Report [36] emphasises that taking risks is what companies do. It is the justification for profit and therefore the identification and assessing of risks is required so that the risks are appropriately managed.

A company should craft a strategy considering their relationship with their various stakeholders. An important aspect of this strategy is managing the uncertainty of future events i.e. managing and containing the risks to an acceptable level. The board of directors should consciously attempt to *build* and *safeguard* trust between them and their investors.

Todd [35] researched trust in the technical arena, specifically focusing on e-commerce. He divided trust into two domains and had subsections in each domain. Todd based his research on Gerck's work [37]. Gerck appears to have originally divided trust into these two domains, *establishing* and *ensuring* trust. Additionally, Gerck focused on trust and risk refinement as a means of reducing uncertainty.

For the purpose and focus of this paper, the domains have been renamed to *Building* and *Safeguarding* trust and the subsections have been modified accordingly.

Appendix A

From the study of the concept of trust it appears that one builds trust over time and then one needs to safeguard trust due to its fragile nature. The following are points (Table 1) which must be taken into account when one considers building and/or safeguarding trust.

Table 1. Building and Safeguarding Trust.

Building Trust	**Safeguarding Trust**
Benevolence/Openness	Risk Management
Ability/Competence	Security Safeguards and Controls
Integrity/Predictability	Compliance
Constant Communication	Recourse Mechanisms
Ethics	Governance
Assurances	'Assurances'

A company, in their strategy, should attempt to mitigate their risks to an acceptable level by reducing the value of opportunistic behaviour from occurring. Moreover, information security audits should be preformed to assure that the technical side of security is adequate as security helps to safeguard trust. Additionally, assurances help to establish trust in the level of confidence placed in the information. The assurances establish a more accurate level of trust *(the truth)* as to the condition of security safeguards and controls. To refer back to the Stag Hunt/Assurance Game, it is the assurances provided by one hunter to the other that keep them *'confident'* that both parties are committed to the hunt. If not, insecurities 'creep' in and alternatively a hunter may decide to hunt a rabbit and the Stag Hunt collapses. Establishing trust sets a level of confidence.

5. Conclusion

Trust and information sharing between the various company stakeholders has taken place since formal commerce began. The information's integrity is of utmost importance, especially the information found within financial statements. This information needs to be trusted. However, the various stakeholders have their own goals and motivations in addition to the shared goals. Conflicts of interest arise and each party is vulnerable. Each also needs to trust the other to have integrity, benevolence, and ability. Companies should have a trust strategy to guide them in building and safeguarding trust, with independent and objective assurances being part of this strategy.

To have a positive outcome, trust needs to increase and uncertainty needs to be reduced to an acceptable level. This could be through assurances provided by auditors *validating* the *reliability* and *accuracy* of the information (the auditors report on the system of internal controls and the accuracy of the financial statements) or through evolving relationships (as discussed in game theory). *To avoid unfavourable behaviour, uncertainty needs to be contained and the level of trust needs to surpass the perceived risks.* This will ensure that a relationship will flourish. Within a

competitive society, the various company stakeholders cannot enter into partnerships with blind trust, believing that everyone will do the right thing [38].

The development of cooperative behaviour and mutual trust should be a goal of all company stakeholders. One cannot escape that trust and controls affect confidence and is the acceptance of a degree of insecurity (as shown in Fig. 2). In conclusion, both *"technical competence"* and *"good intent"* are required to ensure security [1]. Therefore, *confidence in information security management requires trust and trust requires information security to help safeguard it.*

References

1. Camp, L.J.: Designing for Trust. In: Falcone, R., Barber, S., Korba, L., Singh, M., (eds.): Trust, Reputation, and Security: Theories and Practice. Springer-Verlag; Berlin Heidelberg New York (2002) 15-29
2. Ratnasingham, P., Kumar, K.: Trading Partner Trust in Electronic Commerce Participation. (2000) http://portal.acm.org/citation.cfm?id=3598
3. King II Report: King Report on Corporate Governance for South Africa. Institute of Directors in Southern Africa (2002) 17-19
4. Handfield, R.B., Nichols Jr., E.L.: Supply Chain Redesign: Transforming Supply Chains into Integrated Value Systems. Financial Times Prentice Hall, New Jersey (2002)
5. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not So Different After All: A Cross-Discipline View of Trust. Academy of Management Review. Vol. 23(3) (1998) 391-404
6. Johnson-George, C., Swap, W.C.: Measurement of Specific Interpersonal Trust: Construction and validation of a scale to assess trust in a specific other. Journal of Personality and Social Psychology. Vol. 43(6) (1982) 1306-1317
7. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management Review. Vol. 20(3) (1995) 709-734
8. Pearce, W.B.: Trust in interpersonal communication. Speech Monographs. Vol. 41(3) (1974) 236-244
9. Berger, C.R., Calabrese, R.J.: Some Explorations in Initial Interaction and Beyond: Toward a developmental theory of interpersonal communication. Human Communication Research. Vol. 1 (1975) 99-112
10 Berger, C.R.: Communicating Under Uncertainty. In Roloff, M., Miller, G. (eds.): Interpersonal Processes: New directions in communication research. Sage, Newbury Park USA (1987) 39-62
11 Mishra, A.K.: Organizational Responses To Crisis: The centrality of trust. In Kramer, R.M., Tyler, T.R., (eds.): Trust in organizations: Frontiers of theory and research. Sage, California (1996) 261-287
12 Abrams, L.C., Cross, R., Lesser, E., Levin, D.Z.: Nurturing Interpersonal Trust in Knowledge-sharing Networks. Academy of Management. Vol. 17(4) (2003) 64–77
13 Larzelere, R.E., Huston, T.L.: The Dyadic Trust Scale: Toward understanding interpersonal trust in close relationships. Journal of Marriage and the Family. Vol. 42 (1980) 595-604
14 Gefen, D., Rao, V.S., Tractinsky, N.: The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarification. IEEE Computer Society (2002) http://csdl.computer.org/comp/proceedings/hicss/2003/1874/07/187470192b.pdf
15 Von Neumann, J., Morgenstern, O.: Theory of Games and Economic Behaviour. Princeton University Press, Princeton USA (1953)
16 Kimbrough, S.O.: Foraging for Trust: Exploring Rationality and the Stag Hunt Game. (2005) http://opim.wharton.upenn.edu/~sok/sokpapers/2005/itrust-2005-final.pdf

Appendix A

17 Murphy, P.: Game Theory Models for Organizational/Public Conflict. Canadian Journal of Communication. Vol. 16(2) (1991) http://info.wlu.ca/~wwwpress/jrls/cjc/BackIssues/16.2/ murphy.html
18 Hayes, F.: Is Game Theory Useful for the Analysis and Understanding of Decision Making in Economics? (2005) http://www.maths.tcd.ie/local/JUNK/ econrev/ser/html/game. html
19 Khare, R., Rifkin, A.: Weaving a Web of Trust. (1998) http://www.w3j.com/7/s3. rifkin.wrap.html
20 Axelrod, R.: The Complexity of Cooperation: Agent-Based Models of Competition and Collaboration. Princeton University Press, New Jersey (1997)
21 Zand, D.E.: Trust and Managerial Problem Solving. Administrative Science Quarterly. Vol. 17(2) (1972) 229-239
22 Clarke, T.: Theories of Corporate Governance: The Philosophical Foundations of Corporate Governance. Routledge UK (2004) 11
23 Kydd, A. H.: Trust and Mistrust in International Relations. Princeton University Press, Princeton USA (2005) 7-12
24 Axelrod, R.: The Evolution of Cooperation. Basic Books, New York (1984)
25 Partington, A. (ed.): The Oxford Dictionary of Quotations, 4th ed. University Press, New York Oxford (1996)
26 Humphrey, J. Schmitz, H.: Trust and Inter Firm Relations in Developing and Transition Economies. Journal of Development Studies. Vol. 34(4) (1998) 33-61
27 Noorderhaven, N.G.: Opportunism and Trust in Transaction Cost Economies. In: Groenewegen, J., (ed.): Transaction Cost Economics and Beyond. Kluwer Academic, Boston (1996) 105-128
28 Luhmann, N.: Familiarity, Confidence, Trust: Problems and Alternatives. In: Gambetta, D.G., (ed.): Trust: Making and Breaking Cooperative Relations. Basil Blackwell, New York (1988) 94-107
29 Limerick, D., Cunnington, B.: Managing the new organization: A Blueprint for Networks and Strategic Alliances. Jossey-Bass, San Francisco (1993)
30 Camp, L.J.: Trust and Risk in Internet Commerce. The MIT Press, England (2000)
31 Greenstein, M., Vasarhelyi, M.: Electronic Commerce: Security, Risk, Management and Control, 2nd ed. McGraw-Hill, New York (2002)
32 DeMaio, H.B.: B2B and Beyond: New Business Models Built on Trust. John Wiley & Sons, USA (2001)
33 Cox, R., Marriott, I.: Trust and Control: The Key to Optimal Outsourcing Relationships. Gartner database (2003)
34 Fukuyama, F.: Trust: the Social Virtues and the Creation of Prosperity. Free Press USA (1996) 27
35 Todd, A.: The Challenge of Online Trust: For online and offline business. (2005) http://www.trustenablement.com/trust_enablement. htm#RiskManagement
36 Turbull Report. Internal Control: Guidance for Directors on the Combined Code. The Institute of Chartered Accountants in England & Wales (1999/2005)
37 Gerck, E.: End-To-End IT Security. (2002) http://www.nma.com/papers/e2e-security.htm
38 Bavoso, P.: Is Mistrust Holding Back Supply-Chain Efforts? Optimize, and InformationWeek (2002) http://www.optimizemag.com/printer/014/ pr_squareoff_yes.html

Acknowledgement: The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

Appendix B

Computers & Security (2005) **24**, 604–613

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Real-time information integrity = system integrity + data integrity + continuous assurances

Stephen Flowerday [1], **Rossouw von Solms***

Department of Information Technology, Faculty of Engineering, Nelson Mandela Metropolitan University, P.O. Box 77000, Port Elizabeth 6031, South Africa

KEYWORDS
Information integrity;
Internal controls;
Risk management;
Information security management;
Assurance on demand

Abstract A majority of companies today are totally dependent on their information assets, in most cases stored, processed and communicated within information systems in digital format. These information systems are enabled by modern information and communication technologies. These technologies are exposed to a continuously increasing set of risks. Yet, management and stakeholders continuously make important business decisions on information produced in real-time from these information systems. This information is unaccompanied by objective assurances as the current auditing procedures provide assurances months later. Therefore, risk management, including a system of internal controls, has become paramount to ensure the information's integrity. A system of internal controls, including IT controls at its core, help limit uncertainty and mitigate the risks to an acceptable level. Auditors play an increasingly important role in providing independent assurances that the information system's infrastructure and data maintain their integrities. These assurances include proposed new methods such as continuous auditing for assurance on demand.

Introduction

Companies operate in increasingly competitive environments and their information resources play a major role in enabling them to achieve their strategies and objectives. Therefore, it is imperative that the information that a company's directors, managers, employees and various stakeholders base their decisions on, has its integrity intact. The problem occurs when the decisions are made in real-time with real-time information being available. Yet, current methods of producing independent and objective assurances provide 'historic' assurances as the transactions occurred months before. Thus, the decisions made by stakeholders could be flawed due to the condition of the information that their decisions are based on.

* Corresponding author. Tel.: +27 41 5043604; fax: +27 41 5049604.
E-mail addresses: sflowerday@telkomsa.net (S. Flowerday), rossouw.vonsolms@nmmu.ac.za (R. von Solms).
[1] Tel.: +27 43 7352226.

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.08.004

Information security is liable for the information's integrity (NIST 800-53 Publication, 2005; ISO/IEC 17799, 2000). Subsequently, information integrity requires both system integrity and data integrity (Boritz, 2004). Management, as part of their risk assessment process, is required to consider the risks to the company's information assets. Once the threats have been identified, risk mitigation needs to take place so that the risks are contained and are at an appropriate level.

The objective of this paper is to present a method whereby a company can provide the various decision makers with *assurance on demand* by verifying the information's integrity in real-time. This will be done by; firstly, emphasizing the important role that information plays in business decisions today. The importance of information security and particularly information integrity will be highlighted. Secondly, the important role that risk management performs in this regard will be discussed. Thirdly, the important role that internal controls play in ensuring information integrity will be analyzed, followed by the important role that auditing plays in providing assurances as to the integrity of the information. Lastly, the need of continuous auditing will be argued. Automating the audit process is a possible solution to providing *assurance on demand*.

Information

''Information is the oxygen of the modern age.'' (Ronald Reagan, past President of the USA). The world has moved into the *information economy*, an economy based on the exchange of knowledge and services rather than physical goods and services (Australian Government, 2001). Reliable information has truly become crucial to effective decision-making and meeting company's strategies and objectives. This section examines information assets, followed by information security and information integrity.

Information assets

Information held by a company's information systems is among the most valuable assets in the company's care and is considered a critical resource, enabling the company to achieve its objectives. Accordingly, it is stressed that IT products or systems ought to perform their functions whilst exercising appropriate control of this digital information and to ensure it is protected against accidental or deliberate *dissemination*, *modification*, or *loss* (Common Criteria, 2004; Ward and Peppard, 2002). The NIST 800-53 Publication (2005) includes in their assessment of risk a more holistic definition, which includes *access*, *use*, *disclosure*, *disruption*, *modification*, and *destruction* of information.

In fact, it has become so important to protect a company's digital information that the board itself has a fiduciary *duty of care* to ensure that information assets are properly protected (King II Report, 2002; Sullivan, 2000; Turnbull Report, 1999). In addition to the duty of care, there is the legalistic responsibility of compliance with laws and regulations (Westby, 2004).

The Brookings Institute's research and Baruch Lev's analysis of the Standard & Poor's 500 companies (Lev, 2001) suggested that by the late 1990s, on average, 85% of the market value of companies resided in intangible assets (brands, reputation, information, human capital) — *''the largest part of those intangibles being information.''* The remainder of the company's value, approximately 15%, resided in tangible assets (buildings, factories, vehicles).

There has been a significant shift in the valuation of companies from the early 1980s to the late 1990s as the world has advanced into the information economy, as shown in Fig. 1. One of the driving forces behind this shift in market valuations of companies could be the need for increased investment performance. However, regardless of what the driving forces may be; to ensure that information retains its worth it needs to be secured and the users need to have confidence when basing their decisions on the information.

Information security

Information security is an all or nothing proposition. For example: are the horses in the field 75% secured if a fence only exists on three of the four sides? Obviously the horses are not secured. In

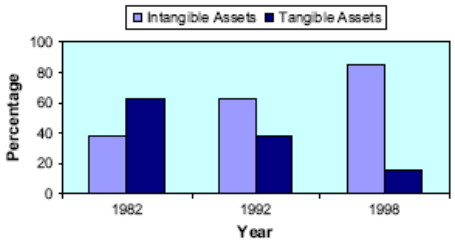

Figure 1 Percentage of company market value related to tangible and intangible assets (Brookings Institute & Baruch Lev's Analysis).

Appendix B

securing information assets and conducting business electronically, it raises information security from a technical issue to a business issue (Dan van Mien and Green-Armytage, 2002). This highlights the need of *"embedding risk and control"* within the culture of the company (Wilson, 2002).

In accordance with the above statement, information security has in fact become a governance challenge and therefore requires all levels within the company to be conscious of the vulnerabilities and risks facing the company (Conner et al., 2004; Conner and Coviello, 2004). This has been accentuated by many governments around the world in passing new legislation concerning the safety of information.

The objective of information security is *"the protection of the interests of those relying on information"* (Horton et al., 2000). To illustrate the importance of this, the AICPA's (2005) Top Technologies Survey showed that for the third consecutive year America's number one technology concern is *information security*.

The NIST 800-53 Publication (2005) points out that information security is preserving the *availability*, *confidentiality* and *integrity* of the information system resources. This is in harmony with ISO/IEC 17799 (2000), which serves as a sound security standard for many companies. ISO/IEC 17799 has information *integrity* as one of the three central pillars of securing corporate information assets along with *confidentiality* and *availability*. It is also stated within this standard that assurance is attained through controls that management creates and maintains within the company.

For the rest of this paper, information security will be considered from a control perspective. As highlighted by GTAG (2005) information security is an integral part of all IT controls and applies to both data and infrastructure.

Information integrity

Information today often exists in electronic form; hard copies or paper trails are disappearing relics of a previous era. Personal identifiers, i.e. signatures, are losing the paper and ink elements that have for centuries been the basis for trust and controls (Horton et al., 2000). Thus far, digital and electronic signatures are not yet as *trusted* as the paper and ink version even though they are legally accepted in many countries. The reason could be that it is difficult to prove who was using the machine/computer when the document was signed.

Vasarhelyi's (2003) notion of the *"electronization of business"*, where he points out the absorption and integration of technology into business processes, highlights the consequent changes this causes to business practices. This notion stresses the flow of electronic information within the company or industry value chain. These automated business processes often extend beyond the borders of a company and are indirectly linked to every online computer within the world. Due to the ubiquitous nature of public and private IT networks and ultimately the Internet, this connectivity introduces additional threats to companies and to the information held in electronic form within companies.

For management to rely on the information within the information systems, assurances need to be provided that the information's integrity has not been compromised, intentionally or unintentionally. Nevertheless, today it is not enough to provide assurances months later, it needs to be in real-time. The information has its integrity only when the accuracy, completeness, timeliness, validity and processing methods are safeguarded (Boritz, 2004; Carlson, 2001; NIST 800-12 Handbook, 1995). According to the IT Governance Institute (Boritz, 2004) integrity means unimpaired or unmarred condition. Applied to information, *"integrity is the representational faithfulness of the information to the condition or subject matter being represented by the information"*.

Information integrity is a narrower concept than information quality. However, it is a broader concept of data integrity (Boritz, 2004). Data are considered to be the raw material used to create a finished product ready for use, i.e. information. It is important to note that besides the data, information integrity is dependent on system integrity. In other words, information integrity can be no better than the integrity of the system processing the data or information, although it can be worse (Boritz, 2004; Woodroof and Searcy, 2001).

A system demonstrates processing integrity if *"its outputs fully and fairly reflect its inputs, and its processes are complete, timely, authorized and accurate"* (Boritz, 2004). To emphasize the two aspects, a system may have integrity but if the data it processes lack integrity at the time the system receives it, then the data will continue to lack integrity when it is transferred to its destination or transformed into information. Thus, to be confident that information, which important business decisions are based on, is trustworthy, both the input data and the processes that are used to produce the information, are properly protected. Protection normally comes in the form of internal controls that result from a thorough risk management process. Risk management therefore plays an important function in ensuring information integrity.

Appendix B

Risk management

Managing information risks and practicing due care are essential to any company (Horton et al., 2000). Risk management takes on a new emphasis today with regulations such as The Sarbanes–Oxley Act (2002) and The New Basel Capital Accord (2004), emphasizing internal controls, transparency and accountability. These regulations go further than before, requiring transparency in the operational processes and the data that make up financial statements.

Management needs to decide how to apply resources to manage the company's risk and the auditors should be in agreement (Hunton et al., 2004). The risk management process attempts to balance risk against the needs of the company (Peltier, 2001). The goal should be to mitigate the risk to an adequate level as no company can afford the resources to control risk to a zero level (Greenstein and Vasarhelyi, 2002; Peltier, 2001; NIST 800-53 Publication, 2005). Two approaches of assessing risk are discussed in this section.

Threats, vulnerabilities and probabilities

One approach is to identify threats, associated vulnerabilities and the probabilities of occurrence. A formula can assist in the decision-making process when determining the *cost* of the risk. Firstly, estimated values need to be assigned to the *Likelihood of the Loss (%) (probability)* and *Loss from the Specific Risk ($) (vulnerability)*. The expected value of risk is calculated as follows:

Expected Value of Risk
= Estimated Loss from Specific Risk ($)
× Likelihood of Loss (%)

Theoretically management should be willing to spend an amount equal to the *Expected Value of the Risk (threat)* to control it, or purchase insurance to offset the loss (Hunton et al., 2004). The problem with this approach is that if one takes this quantitative perspective, at times extreme numbers are produced that lack legitimacy. Consider, for example, the 11th September 2001 World Trade Center disaster in New York. These are not actual figures but are merely to illustrate the following example.

The probability of the occurrence is approximately one million to one and the loss due to the probability occurring was approximately five billion dollars. The resultant Annual Loss Expectancy (ALE or Expected Value of the Risk) would therefore be $5000, but with an ALE of $5000 it is unlikely that any serious security countermeasures would be put in place. Yet the result of this disaster was devastating. Therefore, this risk assessment approach in this case was meaningless. (3.1 example, personal communication, Jason Taule, October 2004).

Although quantitative data may be available for some disasters (earthquakes, floods, etc.) there is less available on situations such as a 'cracker' breaching a network and taking down a mission-critical system. Therefore, *likelihood* data provide greater utility than *probability*.

Risk indicators

This approach uses risk indicators associated with specific processes or technologies. The risk indicators point to a need for controls. Hunton et al. (2004) contend that a company can note the presence or absence of risk indicators for each IT process, and then choose to control them or not, depending on an analysis as to whether or not the risk is acceptable. The findings of the risk analysis will point to the need for a control objective (internal control).

This approach is process-based and is the method that COSO advocates. It can be explained in a more practical way by considering a process, its *inputs* and the desired *outputs*. Along the way there are various mechanisms (activities and tasks) which are applied to the inputs so that the desired outputs are achieved. However, the process is exposed to various risks, which are to be mitigated or managed to an acceptable level by introducing controls.

Stephen Katz (Spafford, 2004), former CISO of Citibank, explained that IT controls do not slow the process down but are like brakes on a car. The driver is actually able to travel faster with brakes than without brakes because the driver is able to keep the car under control. In addition, the car can be stopped much more rapidly and safely if required. Therefore the purpose of risk management is the identification of a system of internal controls that become the foundation to information integrity.

Internal controls

The safeguards that are put in place to ensure that the company's internal information is accurate are referred to as internal controls. Companies have, as part of their risk management, a system of internal controls that are intended to counteract

Appendix B

the inherent risks. Lindberg (2005) points out that internal controls can take the form of operational, financial, or administrative controls.

Overview of internal controls

The COSO (1992) Internal Control Framework, which is widely accepted and used extensively, defines internal controls as a process influenced by a company's directors, management and other personnel. It indicates that internal controls are designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Included in the COSO (1992) Internal Control Framework are five interrelated components which are integrated within the management process. These components vary in procedure and structure from company to company as they are adapted and customized to meet each company's needs and objectives. It should be noted that each one of these five components relates to the three COSO categories above.

These five components are:

- *Control environment*: this is the *''tone at the top''* and is management's attitude towards internal controls. This influences whether the company, i.e. its employees, are control conscious or not.
- *Risk assessment*: this is an important part of internal control. Every company faces a variety of internal and external sources of risks. The COSO-ERM (2004) framework provides companies with guidance in developing plans to identify, measure, evaluate, and respond to risks.
- *Control activities*: these are policies and procedures that are specific to internal controls. They ensure that management's directives are carried out and risks are addressed to enable the company to achieve its objectives. They occur throughout the company at all levels and in all functions.
- *Information (processing) and communication*: relevant information is needed by employees within the company to ensure that strategies and objectives are met as they carry out their responsibilities. This may be internal information within the company or external sources of information from suppliers, customers, shareholders, etc. In addition there is a need for effective communication in the broader sense, such as flowing up, down and across within the company.
- *Monitoring*: continuous monitoring of the internal control system is necessary. This assesses the quality and effectiveness of the system's performance over time.

Strong internal controls increase the probability that transactions are recorded correctly, therefore fraud should not occur and the financial information should be reliable. Establishing and maintaining a system of internal controls is the responsibility of management (Hunton et al., 2004; Braiotta, 2002; Horton et al., 2000; COSO, 1992). In addition, internal auditors should make recommendations to management for improvements in the controls or procedures but they are not responsible for the system of internal controls.

IT controls

Information technology provides opportunities for growth and competitive advantage for companies. However, it also provides the means and tools for threats to exploit vulnerabilities, be this from outside attackers or from trusted insiders. Fortunately, IT can also provide protection from threats. IT controls do not exist in isolation but form part of the overall system of internal controls (GTAG, 2005), which in turn is an integral part of enterprise risk management (COSO-ERM, 2004). These IT controls promote reliability and efficiency and allow the company to adapt to changing risk environments.

IT controls have two significant elements (GTAG, 2005):

- The automation of business
- The control of IT

Hence IT controls support governance and business management as well as provide general and technical controls over policies, processes, systems and people that comprise IT infrastructures (GTAG, 2005). These include the processes that provide assurances for information and assist in mitigating the associated risks.

The COSO-ERM (2004) framework classifies IT controls as either *general* or *application* controls.

- *General controls*: these are also known as general computer controls, information technology controls and infrastructure controls. They include controls over security management,

Appendix B

software acquisition, development and maintenance. They support the functioning of programmed application controls and are the policies and procedures that ensure the continued operation of computer information systems, such as backup, recovery, and business continuity.

- *Application controls*: these pertain to the individual business processes, application systems or programmed procedures in application software. Also covered are the related manual procedures designed to ensure the completeness and accuracy of information processing. Examples include: data edits, balancing of process totals, transaction logging, error reporting and manual procedures to follow up on items listed in exception reports.

The function of a control is relevant to the assessment of its design and effectiveness (GTAG, 2005). Therefore, controls are often categorized into three groups: *preventative*, *detective* and *corrective* controls. CobiT's (2000) Detailed Control Objective DS5.19, titled *''Malicious Software Prevention, Detection and Correction,''* is a good example that illustrates how these controls work together. This control objective deals with malicious software, such as viruses, worms and Trojan horses. Business and IT management should have an adequate system of controls established across the company to protect the information systems from malicious software.

The control procedures should include preventative, detective and corrective controls specifically for malicious software and should incorporate incidence response and reporting. The following are examples of these three control categories:

- *Preventative-controls* prevent unwanted things from happening. For example, CobiT's Audit Guidelines stress, *''all software acquired by the organization is checked for viruses prior to installation and use''*.
- *Detective-controls* monitor activity to determine if the preventive controls have failed. For example, CobiT's Audit Guidelines state, *''users have received instructions on the detection and reporting of viruses, such as sluggish performance or mysterious growth of files''*.
- *Corrective-controls* return the condition back to the expected state. In other words, if a virus did corrupt a system the control would be to reload the applications and the backup or good image to restore the system to the expected state.

Control standards, frameworks, models and guidelines

There have been various control standards, frameworks, models and guidelines developed and proposed over the years. This paper will refer to these collectively as *standards*. However, once a company has completed its risk analysis process it needs to design its own customized control framework (providing guidance, policies and processes) to address its risks. Once the company's control framework has been designed and agreed upon, the company should build an internal control system (the interactive pieces that enable the operation of the framework).

A few standards/guidelines which assist a company in setting up their own internal control framework are: COSO, CobiT, ISO/IEC 17799, ITIL. In many instances a company will use a combination of, or parts from, a few of these standards in designing their own control framework (Oud, 2005; Spafford, 2004). Fig. 2 illustrates how these standards can complement each other as they tend to focus on different areas. Auditors use these standards extensively when evaluating internal controls.

Once an internal control system is operational, a real-time monitoring system of the controls should be in place for management. Such a system is used by an increasing number of companies, the early adopters, each year. This monitoring *overlay* assists management by assuring them that their checks and balances are in place within their business processes. This system also reassures them that their business transactions are sound and the risks are contained. One should not assume that because the company has created an adequate set of internal controls that the controls are always working properly. It is very important that internal controls are continuously being checked for efficiency and operational effectiveness.

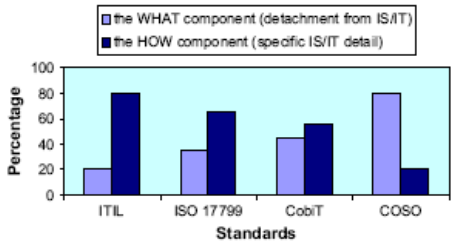

Figure 2 A general guide that illustrates the standard's tendency towards IS/IT or business.

Appendix B

Auditing

In recent years, auditors have shifted their approach and are now using their expertise gained over the decades, to controlling risk. Auditors have moved from a control-based audit model to a risk-based model (Hunton et al., 2004). Rather than just controlling, auditors evaluate risks related to the company's strategy and objectives by selecting cost-effective controls that best mitigate the company's risks. However, it appears that the auditing profession may be making another shift from historic *ex-post* audits to near real-time audits.

With the Sarbanes–Oxley Act calling for reporting to be done on a *''rapid and current basis''*, this leads not only to near real-time reporting but also to near real-time assurances (Alles et al., 2005). Anderson (2005), Senior Vice President – Member & Public Interests of AICPA described the business-reporting model of the future as *''online, real-time disclosure''*. He continues by pointing out that users want *''data on demand''* and more relevant and up to the minute information to assist in better decision-making.

Fig. 3 is a high-level flow chart that illustrates the management and auditing processes. It shows that management is responsible for the system of internal controls and that the auditors will audit both the system of internal controls and the financial data as well as information. Bear in mind that to have information integrity, both the system and the data need to have integrity.

The responsibility of the internal auditors is to give management an independent, objective and fair view of the organization's activities. In addition, the auditors meet on a regular basis with the audit committee to address management, control and assurance issues (Hunton et al., 2004; Cangemi and Singleton, 2003; Horton et al., 2000).

The audit profession has taken advantage of the advances in technology and has developed audit tools and techniques. These allow the auditors to examine all of the company's records and not just a sample, if they so wish. CAATTS (computer assisted audit tools and techniques) and GAS (generalized audit software) enable the auditor to perform data extraction and analysis more efficiently and thereby increase the effectiveness of the audit and the productivity of the auditor.

CAATTS can be separated into two groups: one that focuses on audit *tools* and the other on audit *techniques*. The tools (GAS: expert systems, statistical analysis, etc.) comprise software that increases the auditor's productivity and ability to manage the audit. The techniques (data query models, embedding audit modules, test decks, etc.) validate applications, verify data integrity and test the effectiveness of the internal control system (Hunton et al., 2004; Cangemi and Singleton, 2003). Today, knowledge that your information has its integrity intact is not enough, unless assurances are provided in real-time.

Continuous auditing

Even with the advances in the auditing tools and techniques, the auditors are still providing the assurances months after the transactions have occurred. With real-time information systems and decision makers wanting up to the minute information, there is an even greater need for continuous auditing and assurance on demand. Continuous auditing is defined as (CICA/AICPA, 1999): *''a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter''*.

Continuous auditing technologies could run continuously in the *background* within the company's information systems in a similar manner that virus-scanning programs do (Hunton et al., 2004). Onions (2003) claims that the concept *''electronization''*, which was introduced by Vasarhelyi, has a natural outcome for the audit process to become electronized.

According to The Center for Continuous Auditing (Texas A&M University, 2005), the future audit processes will likely encompass auditors using interrogative software in performing their audit procedures and embedding audit modules into the company's IT environment. It is stated that they feel this will be necessary because *''transactions lose their identity during processing''* and auditing these transactions to determine their validity will require real-time audit processes. This will assist in providing assurances on demand.

Fig. 3 is a high-level view of the entire process. It starts with a *lack of trust* being found in published financial statements. This has resulted from the accounting scandals of the likes of Enron, WorldCom, Tyco, Parmalat, and Ahold, to name a few. The rush to restore investor's and stakeholder's confidence has spawned a pile of regulations and laws, such as Sarbanes–Oxley. Nonetheless, to restore trust is not an easy task. The same elements that restore trust are the same elements that reduce risk.

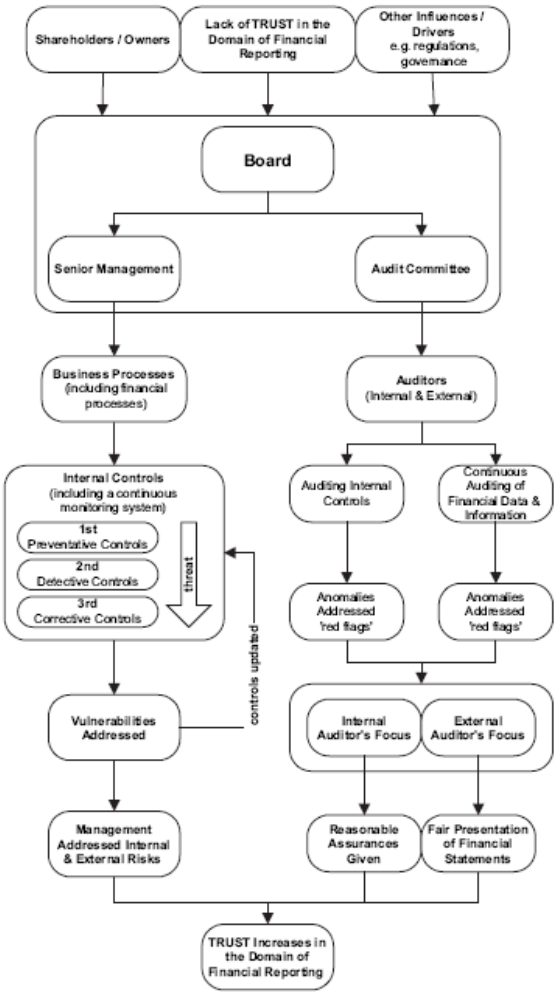

Figure 3 High-level flowchart illustrating the management and audit processes.

As pointed out by Cox and Marriott (2003) confidence has both trust and control as components. Therefore, to restore confidence one needs to find the right balance between trust and control. Fig. 3 highlights the need for a system of continuous monitoring and continuous auditing to provide the required assurances in real-time.

Therefore, to ensure that business decisions are based on *quality* information, a system of internal controls needs to be in place to provide, amongst others, integrity to the information. For these controls to be continuously effective, the controls need to be audited to ensure operational efficiency and effectiveness. As information is required on a continuous basis, these audit processes must be available on demand. Thus, a process of continuous auditing is required to provide information integrity assurances on demand.

Conclusion

Quality information is essential for a company's success. However, the information cannot have quality if it does not have integrity. To have information integrity a company needs to have

a sound system of internal controls with IT controls at its core. These controls need to limit uncertainty and the risks need to be mitigated to an acceptable level. This is one component of information integrity; the other is data integrity. The auditors have several tools and techniques that assist them in determining whether the data have its integrity or not.

This dual-pronged process approach covered in this paper and summarized in Fig. 3, will allow confidence to be placed in the decisions based on real-time information. As indicated in this paper, users want "*data on demand*" and regulations are calling for reporting to be done on a "*rapid and current basis*". In this fast moving corporate environment, where information is crucial to survival, a more automated audit process providing *assurance on demand* by means of continuous monitoring and continuous auditing is the way forward.

References

AICPA. Top Technologies Survey. The American Institute of Certified Public Accountants. Available from: http://www.aicpa.org/download/news/2005_0103.pdf; 2005 [retrieved June 9, 2005].

Alles M, Kogan A, Vasarhelyi M. Real time reporting and assurance: has its time come? Rutgers Business School. Available from: http://raw.rutgers.edu/continuousauditing/; 2005 [retrieved February 4, 2005].

Anderson A. The business reporting model of the future. The American Institute of Certified Public Accountants. Available from: http://www.aicpa.org/pubs/cpaltr/nov2002/supps/edu1.htm; 2005 [retrieved March 23, 2005].

Australian Government. Information management office: glossary. Available from: http://www.agimo.gov.au/publications/2001/11/ar00-01/glossary; 2001 [retrieved May 19, 2005].

Basel II. The new basel capital accord. Switzerland: Bank for International Settlements; 2004.

Boritz JE. Managing enterprise information integrity: security, control and audit issues. USA: IT Governance Institute; 2004.

Braiotta Jr L. Corporate audit committees: an approach to continuous improvement. CPA Journal 2002;73(2).

Cangemi MP, Singleton T. Managing the audit function: a corporate audit department procedures guide. 3rd ed. New Jersey, USA: John Wiley & Sons, Inc; 2003.

Carlson T. Information security management: understanding ISO 17799. Lucent Technologies Worldwide Services. Available from: http://www.netbotz.com/library/ISO_17799.pdf; 2001 [retrieved February 1, 2004].

CICA/AICPA. Continuous auditing. Ontario, Canada: The Canadian Institute of Chartered Accountants; 1999.

CobiT. Control objectives for information and related technology. 3rd ed. USA: IT Governance Institute; 2000.

Common Criteria. For information technology security evaluation: part 1: introduction and general model, (version 2.2 CCIMB). Available from: http://www.commoncriteriaportal.org/public/files/ccpart1v2.2.pdf; 2000 [retrieved January 9, 2005].

Conner B, Noonan T, Holleyman II RW. Information security governance: toward a framework for action. Business Software Alliance. Available from: http://www.bsa.org/resources/upload/Information-Security-Governance-Toward-A-Framework-for-Action.pdf; 2004 [retrieved November 11, 2004].

Conner FW, Coviello AW. Information security governance: a call to action. The Corporate Governance Task Force. Available from: http://www.cyberpartnership.org/InfoSecGov4_04.pdf; 2004 [retrieved October 9, 2004].

COSO-ERM. Enterprise risk management-integrated framework. USA: The Committee of Sponsoring Organizations of the Treadway Commission; 2004.

COSO. Internal control — integrated framework. USA: Committee of Sponsoring Organizations of the Treadway Commission; 1992.

Cox R, Marriott I. Trust and control: the key to optimal outsourcing relationships. Gartner database; 2003 [retrieved March 19, 2004].

Dan van Mien A, Green-Armytage J. Moving to transaction incident management for IS security. Gartner database; 2002 [retrieved July 28, 2004].

Greenstein M, Vasarhelyi M. Electronic commerce: security, risk, management and control. 2nd ed. New York: McGraw-Hill; 2002.

GTAG. Global technology audit guide: information technology controls. USA: The Institute of Internal Auditors; 2005.

Horton TR, Le Grand CH, Murray WH, Ozier WJ, Parker DB. Information security management and assurance: a call to action for corporate governance. The Institute of Internal Auditors. Available from: http://www.theiia.org/download.cfm?file=22398; 2000 [retrieved October 6, 2003].

Hunton JE, Bryant SM, Bagranoff NA. Core concepts of information technology auditing. USA: John Wiley & Sons, Inc; 2004.

ISO/IEC 17799. Information technology — security techniques — code of practice for information security management. International Organization for Standards. Available from: http://www.iso.org/iso/en/ISOOnline.frontpage; 2000.

King II Report. King Report on corporate governance for South Africa. South Africa: Institute of Directors in Southern Africa; 2002.

Lev B. Intangibles: management, measurement, and reporting. Washington D.C., USA: Brookings Institute Press. Available from: http://www.icgrowth.com/resources/documents/Brookings-Lev-Intangibles-01.02.20.pdf; 2001 [retrieved February 10, 2004].

Lindberg D. Corporate governance — the role of the audit committee. Available from: http://www.cob.ilstu.edu/katie/WorkingPapers/CorporateGoverance-Paper1%5B1%5D.isu.doc; 2005 [retrieved July 9, 2005].

NIST 800-12 Handbook. An introduction to computer security. National Institute of Standards and Technology. US Department of Commerce. Available from: http://www.csrc.nist.gov/publications/nistpubs/index.html; 1995.

NIST 800-53 Publication. Information security. National Institute of Standards and Technology. US Department of Commerce. Available from: http://www.csrc.nist.gov/publications/nistpubs/index.html; 2005.

Onions RL. Towards a paradigm for continuous auditing. UK: University of Salford. Available from: http://www.continuousauditing.org/index.htm; 2003 [retrieved November 21, 2004].

Oud EJ. The value to IT of using international standards. Information Systems Control Journal 2005;3.

Peltier TR. Information security risk analysis. USA: CRC Press LLC; 2001.

Sarbanes—Oxley Act. United States of America 107th congress. US Congress. Available from: http://www.sec.gov/about/laws/soa2002.pdf; 2002.

Spafford G. Control framework misconceptions. IT management: network & systems management. Available from: http://

itmanagement.earthweb.com/netsys/article.php/3439901; 2004 [retrieved July 12, 2005].

Sullivan MF. Flunking the duty of care, the four most common mistakes made by directors. Available from: http://www.bricker.com/Publications/articles/157.asp; 2000 [retrieved June 1, 2005].

Texas A&M University. The Center for Continuous Auditing. Available from: http://raw.rutgers.edu/continuousauditing/SummaryofTheCenterForContinuousAuditing.htm; 2005 [retrieved July 19, 2005].

Turnbull Report. Internal control: guidance for directors on the combined code. UK: The Institute of Chartered Accountants in England &Wales; 1999.

Vasarhelyi MA. The electronization of business. Rutgers Business School. Available from: http://raw.rutgers.edu/ecommerce2/; 2003 [retrieved November 5, 2004].

Ward J, Peppard J. Strategic planning for information systems. England: John Wiley & Sons Ltd; 2002.

Westby JR. Information security: responsibilities of boards of directors and senior management. Available from: http://www.reform.house.gov/UploadedFiles/Westby1.pdf; 2004 [retrieved May 29, 2005].

Wilson B, editor. Internal controls assurance: a guide to board level reporting. UK: National Housing Federation; 2002.

Woodroof J, Searcy D. Continuous audit: model development and implementation within a debt covenant compliance domain. Rutgers Business School. Available from: http://raw.rutgers.edu/continuousauditing/; 2001 [retrieved October 14, 2004].

Stephen Flowerday is currently a final year full-time Doctoral student at the Nelson Mandela Metropolitan University in South Africa. His research focus is on providing real-time assurances for information integrity. This is within the domain of corporate governance and information security management. In addition to his studies he lectures part-time and before entering the academic field he had a successful career in management consulting.

Professor Rossouw von Solms is the Head of Department of Information Technology at the Nelson Mandela Metropolitan University in South Africa. He holds a PhD from the Johannesburg University. He has been a member of the International Federation for Information Processing (IFIP) TC 11 committee since 1995. He is a founder member of the Technikon Computer Lecturer's Association (TECLA) and is an executive member ever since. He is also a vice-president of the South African Institute for Computer Science and Information Technology (SAICSIT). He has published extensively in international journals and presented numerous papers at national and international conferences in the field of Information Security Management.

AUDITING

Continuous auditing: verifying information integrity and providing assurances for financial reports

Stephen Flowerday*, Rossouw von Solms, Department of Information Technology, Faculty of Engineering, Nelson Mandela Metropolitan University. [1]

The various stakeholders of a firm have become increasingly reliant upon digital information. This includes financial reports, which are generated from numerous electronic transactions and are recorded in various ledgers. The auditors are expected to audit these financial reports and provide assurances that the information found within these reports has not been compromised, whether intentionally or unintentionally. However, the task of providing the required assurances has become difficult with the fading of the traditional audit trail. Evidence of this is found in the lapses in corporate governance and the recent corporate scandals. A possible solution to this dilemma is Continuous Auditing, which assists in verifying information integrity.

Introduction

Lapses in good corporate governance and accountability have left the various stakeholders wary of the information found in financial reports. The auditing profession's image has been tarnished due to substandard financial reporting and outright fraud. For one to 'trust' the information found in the various financial reports, assurances need to be given that the integrity of the information has not been compromised. With the advances in information technology and the fading of the traditional audit trail, new methods of auditing financial reports and providing assurances of information integrity are desperately needed.

For senior management to comply with new regulations and to restore investor confidence internal controls need to be assessed, evaluated and assurances need to be given. For real-time accounting systems, real-time assurances need to be provided. A 'new' process is emphasized as a possible solution - the Continuous Auditing Process. This process extends beyond the automation of existing auditing methods. The primary focus of this article is to show that continuous auditing can assist in providing assurances that the integrity of the information within financial reports is sound, is intact, and has not been compromised. In addition, the following secondary points are addressed, that of who has the responsibility for the system of internal controls and the integrity of the information. This paper will show how applicable technologies will assist with the primary focus. This discusses technologies such as expert systems, XBRL, and embedded audit modules.

The Corporate Form and the Board of Directors

The corporate form was created as an entity that could outlive any of its members and the board structure was established by law as a vehicle to ensure its continuity and to fix a locus of responsibility for control[30]. The board is generally viewed as fulfilling its formal responsibilities supported by the legalistic argument which indicates that directors must exercise reasonable business judgment in the interests of the shareholders while remaining loyal to the interests of the firm.[3] Although the law gives the board the formal power to control the firm, it provides no specific method to do so.[4,18]

The method whereby the board then chooses to exercise its formal power is through the appointment of a trustee or steward to run the firm, i.e. the CEO.[10,25] The CEO then develops a system of management through which decisions are made and carried out. Nevertheless, regardless of the method of management and controls, the board retains its formal authority over management and is responsible for the firm's conduct and performance .[14,24] To emphasize the point, the day-to-day responsibilities of managing the firm are left to management; however, the board retains ultimate authority and responsibility for the firm's performance.

It should be noted that the firm exists as an entity to provide value for stakeholders.[5] Furthermore, it is stressed by Donaldson,[8] the chairman of the Securities and Exchange Commission (SEC) in the USA, that capital will flee environments that are unstable or unpredictable and that investors must be assured that firms are living up to their obligations. How does the board of directors know if the firm, especially a large diverse or multi-national one, is living up to its obligations as an entity?

The Audit committee

The board has various committees that advise it and report on the firm. Through these committees the board remains informed as to the firm's conduct and performance. One of these committees is the Audit Committee. This committee is defined as a subsection of the board, designated with oversight responsibility to include: (1) finan-

cial reporting, (2) auditing and (3) internal controls. To reiterate, the audit committee is a representative of the full board[7].

As a means of fulfilling its oversight function, the audit committee must ensure that management has fully assessed all of its risk and maintains effective risk management.[5,12] Essentially risk is assumed on both a voluntary and involuntary basis for all firms. The risk analysis part of risk management identifies risks that need to be controlled or accepted. It is important to note that there is also a general assumption that computers cannot ever be fully secured. There is always an element of risk, be it internal, external or threats to the infrastructure of a firm. This residual or inherent risk is based on the notion that additional investment in safeguards and controls will not eliminate this type of risk, or that it is not cost effective to attempt it. This is known as risk acceptance.

IT Business Risk represents a significant involuntary risk given that a firm's information is among its most vital assets and is paramount to the firm's success.[12] The nature of IT business risk, information systems and information assets is that they are woven throughout the fabric of the firm and are embedded in its business processes.[28] This article emphasizes internal controls as an integral part of enterprise risk management, which in turn is part of the broader management process.[5] Management has the responsibility to ensure that the integrity of the information embedded in the business process, and especially the financial process, that make-up the financial reports is untainted. In addition, managers today ought to be aware that an effective system of internal control over financial reporting has its foundation in IT.[13]

The audit committee is to consider the effectiveness of the firm's internal control system, including that of its information systems. The COSO-ERM report[5] has classified information system controls into two broad groupings: General and Application Controls. The report states that these controls, *"combined with manual process controls where necessary, work together to ensure completeness, accuracy, and validity of information."*

The committee is also to understand the scope of the internal and external auditor's review of internal controls over financial reporting. In addition, it is to obtain reports on significant findings and recommendations, together with management's responses. Given that most operational processes, especially those supporting the firm's finances, are automated and use information technology, one cannot emphasize the internal controls for information technology enough. Today it is accepted that IT systems are inextricably linked to the financial reporting processes.[13]

The COSO-ERM report[5] refers to the specific controls within the firm's applications, such as ERP systems, that help to control the processing as Application Controls. These Application Controls are a broad group of controls that *"focus directly on completeness, accuracy, authorization, and validity of data capture and processing"*. Given the enormity of IT business risk, the audit committee would be lacking in its duty of providing due care, pertaining to its oversight function, if it failed to ensure that management did not extensively perform its risk identification, mitigation, and management of all risks.[12]

Breakdown in financial reporting

The recent fraudulent transactions and financial crises created by Enron, WorldCom, Tyco, Parmalat, Ahold and others, have turned the spotlight on corporate governance and financial reporting. As a result the current financial reporting model is being heavily scrutinized and this is evident in the recent significant regulatory reform measures being considered and implemented. The net effect of these 'breakdowns' has left the investor wary and lacking faith in the integrity of published financial reports.

Confidence and trust needs to be reinstalled in the boards of firms and in the auditing profession. To restore trust is not an easy task, seeing that risk and trust appear to be significant variables. Risk, being ubiquitous in nature and evident in economic transactions, needs to be addressed thoroughly. John Shaw[23] succinctly stated, *"One may not manage risk, but one can manage for risk."* This need accentuates the importance of a firm's risk management to include IT business risk and internal controls to help ensure the accuracy of the information in their financial reports.

In response to these and other recent corporate scandals and breakdowns in financial reporting, the Sarbanes-Oxley Act of 2002[22] was passed in the USA in an attempt to help restore investor confidence. The Act further aims to enhance corporate governance and strengthen corporate accountability.[13] This Act has been the most significant piece of securities legislation passed in the USA since the securities acts of 1933 and 1934.[8,16] The Act establishes requirements for the SEC in the USA to establish rules for public firms to comply with. Among these rules and safeguards are the following:

- The CEO and CFO are to certify the firm's internal controls over financial reporting (section 302 of the Act).
- Auditors and management, in their assessment of risks, are to certify the adequacy as well as evaluate and report on the effectiveness of internal controls over financial reporting (section 404 of the Act). There were 582 firms which made "weakness and deficiency disclosures" during their 2004 filing of financial reports in the USA.[1] The majority of these disclosures, 50.1%, were related to financial systems and procedures.
- *"Material changes"* are to be disclosed to the public on a real-time basis. This is broadly defined as all significant internal control design or operational deficiencies that could adversely affect the reported financial information and is to be done for the protection of investors (section 409 of the

Act). It is expressed that this be carried out on a *"rapid and current basis"*. There are those that stress that this section is of utmost importance to the investor and that it will create a challenge for the 'IT' community to comply to, as this requires a dynamic risk monitoring framework.[9] As emphasized, real-time reporting requires real-time assurance.[2,19]

Non-compliance with the Sarbanes-Oxley Act in the USA results in significant penalties for CEOs and CFOs, including monetary fines and/or imprisonment. The USA is not alone in passing legislation in an attempt to improve investor confidence and improve corporate governance. As highlighted, the world securities markets have recognized the need for reform.[8] Donaldson stated that the standards everywhere are being raised to ensure that the investors have the protection they need and deserve. This is evident in regulations that are similar in nature and intent to the Sarbanes-Oxley Act, being considered and passed in many countries; for example, Canada, South Africa, Australia, Singapore and the European Union.

A new business process

For the various senior managers, committees, investors and stakeholders to know that the information and reports they base their decisions on are correct, assurances are needed that the integrity of the information is intact and that the reports are based on untainted data. Orderly processes are now necessary to provide an effective audit trail for the flow of data. Such processes are critical if auditors are to adequately assess strengths and weaknesses in the information security and internal control environments as well as audit transactions in real-time.[29]

Part of the internal auditors' responsibilities is to test management and employees' compliance with the firm's policies and procedures, and to evaluate the adequacy of internal control environment. Conversely, with the increased use of ERP systems and more sophisticated information systems in which the audit trail is not clear, internal auditors may be required to develop new processes, such as continuous auditing for the testing and monitoring of the internal control environment. The Sarbanes-Oxley Act, specifically section 409, has created an increased demand for continuous auditing and the internal auditor may play a key role in this process.[6]

Continuous auditing

Real-time financial reporting is likely to necessitate continuous auditing. One would need to provide continuous assurance about the quality and credibility of the information presented.[21] Continuous auditing is defined by Rezaee et al.[21] as *"a comprehensive electronic audit process that enables auditors to provide some degree of assurance on continuous information simultaneously with, or shortly after, the disclosure of the information."*

Continuous auditing systematically and continually tests transactions using intelligent software tools. The auditor prescribes the criterion and the process identifies anomalies and exceptions for which additional audit procedures should then be performed. Depending on the findings, the auditor may issue a report. The growth of ERP systems, increased bandwidth and use of the Internet, the speed of processing and the globalization of business have all contributed to the development of more intelligent software tools.[21,27] These developments provide management and auditors with the ability to better capture and analyze key data for decisions. The use of intelligent agents, embedded in audit modules to monitor and trigger alarms when unusual transactions or patterns occur, provides management with tools to better monitor business processes.[29]

Warren and Parker[29] claim that these software tools are especially suited for firms with high volume and high-speed applications and which have complex information technology environments (e.g. banks and financial services firms). They feel that in these environments it is necessary to have in place a process, such as continuous auditing, that will not impede the flow of data. Furthermore, the Internet has created an electronic means for providing information to interested parties, such as, investors, regulators and customers on a global real-time basis.[29] It is therefore logical that management will be required to put in place internal controls that protect the integrity of information from unauthorized access or use, and that such measures will become part of the firm's overall monitoring platform.

While the auditing profession has long discussed the concept of continuous auditing, it has remained chiefly in the academic domain. [19,21,29] However, there are strong drivers for this 'new' process and change in auditing methods. Marks[15] pointed out that firms are rapidly installing new technologies that require auditors not only to understand them, but also to assess the risks associated with these technologies. As early as 1989[11] it was recognized that information systems in firms were becoming increasingly complex and the traditional audit trail was disappearing. As a result, internal control and security have become critical concerns.

Vasarhelyi[26] believes that real-time systems will impact on the procedures employed by auditors and suggests a continuous audit process. In addition a new paradigm of auditing needs to be accepted and implemented to match the relentless pace of technological change.[19] Corporate-wide networks enable firms to integrate global manufacturing, inventory record keeping, financial management and informative forms of corporate reporting.[26] Furthermore Vasarhelyi notes that the exponential growth of online retailing, securities trading and procurement systems again emphasizes the need for continuous auditing. It was further stated by Vasarhelyi that the evolution of audit thinking, the *"electronization of business"*, the availability of new technologies and the aging of the audit product, all require new thinking in the auditing area.

In December 2002, the American Institute of Certified Public Accountants (AICPA) established the Enhanced Business Reporting Model Committee to migrate the current reporting model to an online, real-time business-reporting framework. This framework will call for continuous assurance of the information being reported.[17] Modern-day business complexity and technology are attributes of firms that suggest auditors will be required to develop new methodologies and processes for auditing. Continuous auditing may be one of the processes developed to respond to these business attributes.

XBRL and continuous auditing

Section 409 of the Sarbanes-Oxley Act refers to reporting done on a *"rapid and current basis"*. To accomplish this, the reports that are generated in a near real-time basis need to be accompanied with assurances that the integrity of the information is intact. Even though technology has advanced and there are methods that compile financial reports on a near real-time basis, the auditing profession has not yet been able to provide assurances that the information within these reports is 100% accurate. Extensible Business Reporting Language (XBRL) is an extension language of XML and is created as a language that can possibly provide seamless continuous financial reporting and which can lead to accurate real-time reporting of financial reports.

XBRL allows tagging of data so that it can be accepted directly into the recipient's database for further analysis (see www.xbrl.org). In addition, XBRL has the capability to populate auditor databases for immediate evaluation by auditors and their automated tools. Following this, statistical methods such as data mining can be used to identify high-risk transactions.[20] XBRL is designed to make it easier to prepare, publish, exchange, acquire and analyse accounting and business related information. Alles et al.[2] argues that section 409 will eventually require assertion and assurances of continuous monitoring of corporate controls and that meta-controls at each process (process assurance) will be used to improve the quality of the data being transmitted from process to process.

The auditing of transactions should be carried out in real-time as business is conducted in real-time.[19] Onions, from the European Center for Continuous Auditing, proposes Extensible Continuous Auditing Language (XCAL). XCAL, together with expert systems, will verify transactions at keystroke entry level and perform a more thorough interrogation of the data in a data mine before assurances are given.

It is proposed that if the data in the sub-ledgers is fraudulently or erroneously entered it will carry through to the general ledger. It is this data that will be used by XBRL from the general ledger in formulating the financial reports.[19] The point being, that the auditor could not report on or give opinions and assurances that the integrity of the data in the general ledger is correct, without going through a process of 'checking' the entries and transactions in the sub-ledgers.

Onions,[19] emphasizes that one should follow the data path from data entry all the way through to the posting in the general ledger. This is a mammoth task to be conducted manually, or with Computer Assisted Audit Tools (CAATS), and that is why the traditional audit takes a sample of transactions for testing. Even using CAATS the testing is done in batch mode and so generally only a sample is tested, or if tested in its entirety it is done after the fact and the reports are historic.

The advantage of continuous auditing is that with the advances in technology, i.e. more powerful processors and increased bandwidth, every transaction can be checked. To increase the quality of the audit, every transaction should be stored in a data mine. The aggregated data is to be trawled by expert systems searching for predefined patterns, heuristically with rules specified by the auditor.[19] This dual pronged approach of checking transactions in a data mine and at keystroke entry is continuous in nature and should provide near real-time assurances that the information in the ledgers has not been compromised.

Conclusion

With the integrity of the information in financial reports being questioned and the shift towards more rapid financial reporting, the auditing profession has had to find new ways of verifying the information in these reports. The audit committee, representing the board of directors, has the responsibility of overseeing that management install adequate internal controls over financial reporting. The relentless advances in information technology have required new methods of 'checking' and providing assurances that the internal controls and the integrity of information is sound. However it still has a way to go.

Continuous auditing and monitoring have increased in importance especially if one considers compliance to the Sarbanes-Oxley Act and others. Auditors should embrace technologies like XBRL and expert systems as they try to meet the needs of firms. In improving the internal controls and thereby the quality and accuracy of information within financial reports, one cannot but help to improve corporate governance and investor confidence. The day of the firm's directors claiming "I did not know" in connection with errors and fraud in their firm's financial reports and getting away with it, should be over.

Author contacts:

*Corresponding author.
Tel.: +27-43-7352226;
fax: +27-43-7481801.
E-mail: sflowerday@telkomsa.net
Postal address: P. O. Box 15520, Beacon Bay, East London, South Africa, 5205

Prof. Rossouw von Solms.
Tel.: +27-41-5043604;
fax: +27-41-5049604.
E-mail: rossouw.vonsolms@nmmu.ac.za

References

[1] 582 weakness, deficiency disclosures made in '04, Compliance Week, http://www.complianceweek.com/index.cfm?fuseaction=article.viewArticle&article_ID=1456, 11 January 2005.

[2] M. Alles, A. Kogan, M. Vasarhelyi, Real time reporting and assurance: Has its time come?, Rutgers Business School, http://raw.rutgers.edu/continuousauditing/, 4 February 2005.

3 M. E. Budnitz, Business reorganizations and shareholders meetings: Will the meeting please come to order, or should the meeting be cancelled altogether?, The George Washington Law Review 58, 1990, pp. 1214-1267.

[4] R. N. Carpenter, Corporate governance, part II: Directors responsibilities, Directors & Boards 29 (3), 1988, pp. 3-6.

[5] COSO, Enterprise risk management-integrated framework, The Committee of Sponsoring Organizations of the Treadway Commission, 2004, pp. 24-26, 64-65.

[6] R. J. Daigle, J. C. Lampe, Responding to the Sarbanes-Oxley Act with continuous online assurance, Internal Auditing 18 (2), 2003, pp. 3-7.

[7] F. T. DeZoort, An investigation of audit committees' oversight responsibilities, A Journal of Accounting, Finance and Business Studies 33 (2), 1997, pp. 208-227.

[8] W. H. Donaldson, U.S. Capital markets in the post-Sarbanes-Oxley world: Why our markets should matter to foreign issuers, London School of Economics and Political Science, speech 25 January 2005.

[9] M. Emery, Monitoring Sarbanes-Oxley Act: Section 409 Compliance, 2020 Governance AB, Stockholm, Sweden, 2004.

[10] E. J. Epstein, Who Owns the Corporation? Management vs shareholders, New York, Priority Press Publications, 1986.

[11] S. M. Groomer, U. S. Murthy, Continuous auditing of database applications: An embedded audit module approach, Journal of Information Systems (spring), 1989, pp. 53-69.

[12] T. R. Horton, C. H. Le Grand, W. H. Murray, T. R. Ozier, D. B. Parker, A call to action for corporate governance, in: Proceedings of the Washington Information Security Summit Conference and regional conferences in Dallas, Atlanta, Chicago, San Francisco, and New York, 2000, pp. 1-20.

[13] IT Control Objectives for Sarbanes-Oxley, The IT Governance Institute, USA, 2004.

[14] King II Report, King report on corporate governance for South Africa, Institute of Directors in Southern Africa, 2002, pp. 79.

[15] N. Marks, The new age of internal auditing, The Institute of Internal Auditors, Florida, http://www.theiia.org/index.cfm?act=home.login&return=doc_id=2738, 2001.

[16] A. D. Morrison, Sarbanes-Oxley, corporate governance and operational risk, in: Proceedings of the Sarbanes-Oxford Conference held at Said Business School, University of Oxford, 22 July 2004.

[17] New business reporting model beginning to emerge – timeliness, reliability, transparency to be improved, American Institute of Certified Public Accountants, http://www.aicpa.org/pubs/cpaltr/dec2002/business.htm, 2002.

[18] C. H. Ong, S. H. Lee, Board functions and firm performance: A review and directions for future research, Journal of Comparative International Management 3 (1), 2000.

[19] R. L. Onions, Towards a paradigm for continuous auditing, University of Salford, United Kingdom, http://www.continuousauditing.org/index.htm, 2003.

[20] Y. Rechtman, Continuous auditing and XBRL, The Trusted Professional, NYSSCPA 7 (8), http://www.nysscpa.org/trustedprof/504/tp13.htm, 2004.

[21] Z. Rezaee, A. Shabatoghlie, R. Elam, P. L. McMickle, Continuous auditing: Building automated auditing capability, Auditing: A Journal of Practice and Theory 21 (1), 2002, pp. 147-163.

[22] Sarbanes-Oxley Act, United States of America 107th Congress, http://www.sec.gov/about/laws/ soa2002.pdf, 30 July 2002.

[23] S. J. Shaw, Corporate Governance & Risk, New Jersey, John Wiley & Sons, Inc., 2003, pp. 75, 141.

[24] R. I. Tricker, International Corporate Governance, Singapore: Prentice-Hall, 1994.

[25] S. C. Vance, Corporate Leadership Boards, Directors and Strategy, New York, McGraw-Hill, 1983.

[26] M. A. Vasarhelyi, Concepts in continuous assurance, Rutgers Business School, http://raw.rutgers.edu /continuousauditing/conceptsincontinuousassurance13final.doc, 2002.

[27] M. A. Vasarhelyi, M. G. Alles, A. Kogan, Principles of analytic monitoring for continuous assurance, in: Proceedings of the Fifth Continuous Auditing Symposium held at Rutgers Business School, http://raw.rutgers.edu/continuousauditing/, 2003.

28 J. Ward, J. Peppard, Strategic Planning for Information Systems, England, John Wiley & Sons Ltd., 2002, pp. 59.

29 J. D. Warren, X. L. Parker, Continuous Auditing: Potential for Internal Auditors, The Institute of Internal Auditors Research Foundation, Florida, 2003.

30 M. N. Zald, The power and functions of boards of directors: A theoretical synthesis, American Journal of Sociology 74, 1969, pp. 97-111.

COMPUTERS & SECURITY 25 (2006) 325–331

available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Continuous auditing technologies and models: A discussion

S. Flowerday, A.W. Blundell, R. Von Solms*

Centre for Information Security Studies, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

ARTICLE INFO

Article history:
Received 13 June 2006
Revised 13 June 2006
Accepted 13 June 2006

Keywords:
Continuous auditing
Real-time assurances
Information integrity
Internal controls
Technology-based prevention

ABSTRACT

In the age of real-time accounting and real-time communication current audit practices, while effective, often provide audit results long after fraud and/or errors have occurred. Real-time assurances can assist in preventing intentional or unintentional errors. This can best be achieved through continuous auditing which relies heavily on technology. These technologies are embedded within and are crucial to continuous auditing models.

1. Introduction

In today's fast paced business world, real-time information systems facilitate real-time accounting systems and real-time communication between entities. Current audit practices, while proving adequate, take too long to provide assurances. Current audit practices also uncover intentional and unintentional errors, however, only after it has possibly had a detrimental effect on the organisation. A method of prevention by detecting these errors early is desirable. It is time to provide real-time assurances to decision makers.

Real-time assurances can only be provided by continuous auditing technologies. This paper discusses a range of audit technologies within three continuous auditing models. Each of these models has a different focus and makes use of different technologies. The available technologies, tools and techniques used in continuous auditing, will be interrogated.

The aim of this paper is to reach a conclusion about how a generic, yet comprehensive continuous auditing system could make use of the available tools, techniques and technologies for testing internal control and performing tests on transactions. To achieve this aim, after discussing the history and definition of continuous auditing the reasons for using continuous auditing systems will be explored. Once this is clarified, the tools and techniques necessary to implement continuous auditing are discussed, these are then placed into context by discussing three prominent continuous auditing models. The three models are then compared in tabulated form, after which possible future technologies are suggested for addressing internal control issues and testing transactions within a continuous auditing system.

2. Definition and history of continuous auditing

There are several differing ideas of what continuous auditing (CA) systems are, and how they work. Each of the models

* Corresponding author.
E-mail addresses: sflowerday@telkomsa.net (S. Flowerday), ablundell@nmmu.ac.za (A.W. Blundell), rossouw@nmmu.ac.za (R. Von Solms).
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.06.004

Appendix D

(discussed later) has their own definition, differing slightly. The most widely accepted definition though, is one released in 1999 and reads as follows: "*a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short time after, the occurrence of events underlying the subject matter*" (CICA/AICPA, 1999). This is the definition used for the purpose of describing continuous auditing throughout this paper.

In the early 1990s, the business environment went through a series of substantial changes. The "Electronization" of business and the proliferation of e-business lead to paperless accounting systems (Bierstaker et al., 2001; Vasarhelyi, 2002). This move towards technologies such as Electronic Data Interchange (EDI) and Electronic File Transfer (EFT) caused the evaporation (or disappearance) of the traditional audit trail. Auditors could no longer look for source documents in paper form and increasingly had to perform tests and gather evidence electronically, thus their audit techniques had to undergo some changes (Bierstaker et al., 2001; Helms and Mancino, 1998).

The trend which caused the disappearance of the traditional audit trail continued and online systems and the Internet created an easier, cheaper way for data to be exchanged between systems. The *html* documents proved to be inadequate as it was difficult to extract and compare data because *html* only describes how data should be presented (Alles et al., 2004). Therefore, a language which could be intelligently manipulated and which would form a standard for data transfer was required. XML (eXtensible Markup Language) adds information about the document's content to its tags, thus it is easy to search, especially if digital agents are used. A subset of XML, XBRL (eXtensible Business Reporting Language) was created to describe business reporting information.

XBRL is useful for preparing, publishing, exchanging, acquiring and analysing accounting and business data, and provides a standardised method for transferring financial reporting information between different software applications (Alles et al., 2004; Srinivas, 2004). XBRL assigns tags to financial information, which allows computers to "understand" the data, while it can still produce human-readable reports. These tags are standardised by rules known as taxonomies. Taxonomies can contain rules (and tags) specific to certain industries or businesses as well as the Generally Accepted Accounting Principles (GAAP) rules. These may be region or country specific though (Pinkster, 2003).

XBRL enables continuous auditing by placing financial data in a format which is not proprietary to any specific software application, allowing any future continuous auditing system access to data on any software platform, running any software (which uses XBRL), in any country.

The concept of continuous auditing has been established in this section, this has explained *what* continuous auditing is. In the next section, *why* continuous auditing is necessary will be explained.

3. Motivation for CA technologies

In real-time accounting systems it has become desirable to have continuous assurances as to the condition of the information's integrity (Flowerday and von Solms, 2005). Furthermore, continuous assurances allow for corrective action to be taken sooner when a problem is found rather than in current auditing scenarios. To quote, "*The focus of the audit will shift from manual detection to technology-based prevention*" (Bierstaker et al., 2001).

Auditors aim to provide management with an opinion on subject matter for which management is responsible. In order to do this he/she will have to *validate* the *accuracy* of financial records and the *reliability* of the systems which store, transport and process those transactions. Looking at accuracy entails checking for fraud and error in transactions. There are well established auditing technologies which can assist in looking for *material* misstatements in financial records. Using these technologies within a continuous auditing system can extend their current effectiveness, as all transactions are analysed in real-time.

When assessing the reliability of the reports produced by the system, the auditor will look at confidentiality, integrity and availability and how this is ensured by the system of internal controls. Technology can be used to assess the internal control systems and see whether they are in line with prescribed norms. In the next section the nature of these technologies will be explored, explaining *how* the aims of continuous auditing can be met.

4. Technology aided tools and techniques

In order to verify that a real-time accounting system is producing reliable and accurate financial information, testing of controls must be done simultaneously with substantive tests of transactions (Helms and Mancino, 1999; Rezaee et al., 2001).

There are various tools and techniques which can aid in the analysis of transactions and internal controls. The tools are required to perform a variety of tasks. They can either be purchased software packages or auditor-designed routines (Rezaee et al., 2001). Collectively these tools and techniques are often referred to as Computer Aided Tools and Techniques or CATTs. An alternative acronym is CAATTs or Computer Aided Audit Tools and Techniques. CATTs have been used by auditors for many years and incorporate a wide variety of technologies, some of which are applicable to continuous auditing. In certain literature these have become known as Continuous Auditing Tools and Techniques. In this paper, "CAATTs" will refer to all of these collectively.

4.1. *Tools and techniques for analysing transactions*

To meet the requirements of an audit it is necessary to verify the accuracy of transactions to reveal fraud or error. Substantive tests of transactions must be performed. These will aim to obtain evidence showing possible material misstatements in the financial statements (South African Institute of Chartered Accountants, 2003). Two types of substantive tests are performed.

4.1.1. *Analytical procedures*

Analytical procedures involve performing comparisons of financial data to establish a relationship, often involving the

Appendix D

calculation of ratios. Analytical procedures not only indicate the possible existence of financial misstatements, they can also reveal how the client's industry and business function. When performed in the final phase of an audit, analytical procedures allow the auditor to comment on the reasonableness of transactions and the ability of the client to continue as a going concern.

CAATTs make analytical procedures more feasible and affordable than before (Rezaee et al., 2001). Many types of analytical procedures are too complex or time-consuming to be done manually. Using CAATTs also means that it has become possible to use larger sets of data when performing analytical procedures.

4.1.2. *Tests of transactions and balances*

The testing of transactions is often performed at the same time as testing controls. Transactions are tested continuously, throughout the financial year. This is done to discover whether material misstatements have occurred. In other words, to see whether erroneous or irregular processing of the transactions has taken place.

Testing transactions continuously throughout the year can help to reduce the number and/or complexity of tests of balances which need to be performed after balance sheet date (Rezaee et al., 2001). Tests done on balances are usually to collect evidence, on which the auditor can ground his or her opinion on fair representation of financial statements (Rezaee et al., 2002). When performing substantive tests of balances, Generalized Audit Software (GAS) tools are often used (Rezaee et al., 2001).

4.2. *Tools used in testing of internal controls and assessing risk*

In order to plan an audit, the auditor needs to be aware of the areas which carry the greatest risk and thus need the most scrutiny. This requires the auditor to look at the adequacy and effectiveness of internal controls within the system. According to the statement on auditing standards No. 80 (AICPA, 1996) CAATTs can be used for this purpose.

Testing of controls should also be ongoing. This allows the auditor to express an opinion as to how reliable the internal control system is. Knowing the reliability of the internal control system is important during the planning phase of an audit. The nature, timing and extent of substantive tests will be decided on accordingly (Rezaee et al., 2001).

In this section, the tools and techniques used for both analysing transactions and testing internal controls were elaborated, in the next section three of the models which use these tools and techniques will be explained.

5. Continuous auditing models

There are several suggested continuous auditing models, most are merely conceptual. Few seem to have been implemented in real-time systems. One of the early models was the Continuous Process Auditing System (CPAS) which was developed at AT&T Bell Laboratories. This is a methodology for internal auditing of large "*paperless*" real-time systems (Varsarhelyi and Halper, 1991). This model appears to have formed a basis for the later models.

In this paper, three of the better known models have been chosen for discussion. These all take somewhat different approaches and make use of different technologies.

5.1. *Continuous auditing building automated auditing capability (Rezaee et al., 2002)*

This is a conceptual framework for a continuous auditing system. It would be capable of running on a distributed client/server network and is also web-enabled for transmitting data to audit workstations. The model involves several steps.

Firstly, data are collected from transactional systems. This is done by linking to tables, via File Transfer Protocol (FTP), storage drives or via modem. The data are then stored on an audit server.

Once on the audit server, data are extracted from a variety of platforms and systems. Data standardisation is therefore required. Standards and formats are developed for storing data in the data warehouse/mart. The data are then transformed by cleaning, validating, restructuring the data and "scrubbing" with business rules.

An enterprise-wide data warehouse is not always needed, as it may be too expensive and complex. Instead, the required data could automatically be fed into several data marts. Data marts contain metadata which details the source transactions and the ETL (Extract Transform Load) process as well as the tests which take place. The metadata may for example include: detailed file definitions, business rules and transaction process flows.

Lastly, standardised tests are created to run within the data mart. The tests are created either to run continuously or at predetermined intervals. The tests are designed to automatically gather evidence and issue exception reports.

5.2. *Towards a paradigm for continuous auditing (Onions, 2003)*

To monitor the integrity of the data, Onions suggests *keystroke level* data examination. This basically involves monitoring database utilities and applications for commands which could cause fraud or error. This model addresses the testing of transactions in two ways.

Firstly, each transaction is audited and reported on as an isolated entity. This is done "*ephemerally*" – the transactions are tested at the time of entry. This is referred to as *transaction level* data examination. It ascertains whether each transaction fits the pre-specified rules for that transaction. These may be business rules or even rules dictating what actions are permissible for certain users. This is done in conjunction with performing certain analytical functions. Computer Assisted Audit Tools could be used. However, these operations would need to be performed on the transactions in real-time rather than batch. After the transaction has been examined it may be added to a data mine for possible further examination.

Secondly, the transactions are examined as a whole over a longer time period (perhaps even years). This examination looks for patterns in the transactions which could together result in fraud. This is known as the *transaction pattern level*

of data examination. Expert systems and rules based criteria would be employed. Rules would be similar to virus definitions and would be available for different industry types.

The problem when attempting to use expert systems is that each software package available has a different data schema. It would be very costly and time-consuming to create expert systems for each application. The solution would be to create a generic master file and transaction layout which could be used regardless of application data schema. This newly defined generic schema for a transaction would allow one expert system to trawl through the data mine. This schema would be defined using eXtensible Continuous Auditing Language (XCAL) which, similar to XBRL, is XML-based.

The model consists of four levels:

1. Transactions and data from various sources are entered for processing.
2. Transactions and keystrokes are mapped to XCAL schemas. This is done in real-time and is captured forensically on a daily basis.
3. Real-time CAATT processing is used to check transactions and keystrokes. Alerts may be sent to an Online Systems Audit Centre (OLSAC). Transactions are stored at this level for a day (but passed to level 4 where they are stored for years).
4. Expert systems look for patterns in the data.

5.3. *Continuous audit: model development and implementation within a debt covenant domain (Woodroof and Searcy, 2001)*

Woodroof and Searcy's model presents a conceptual model of continuous auditing. This model is limited in scope, as it is discussed in relation to debt covenant compliance. The model makes use of web-enabled technologies. It draws attention to the need for a reliable and secure system. The need for the production of *evergreen reports* is also discussed. Evergreen reports are reports which are generated on demand, usually viewed through a web site. The model is based on a database of transactions (journals and ledgers) on the client's system, with a web interface (on the auditors system) for the auditor to use.

This model is implemented in five stages:

1. A request is made for a report.
2. Agents and sensors within the client's system monitor the transaction data for exceptions to pre-specified rules. These exceptions are compared to the auditor-defined rules. This may trigger alarms, and alerts are sent to the auditor. The rules check the reliability of the system (possibly using continuous SYSTRUST), the fairness of the representation of financial reports and compliance to 3rd party contracts (like debt covenant agreements).
3. A digital agent on the auditor's system requests a digital agent on the client's system to retrieve the client's real-time balances of accounts via stored procedures in the client database.
4. If more information is returned than is needed, the digital agent extracts the information relevant to the "contract" (in this case debt covenant compliance). The information is checked for compliance, the actual event or process is checked against an acceptable standard for that event or process. If anomalies occur, these are flagged and the auditor is notified so that he/she may take action.
5. An evergreen report is generated and displayed to the loan officer. This details three levels of assurance. Level 1 is an assurance of reliability. If there is Level 1 exception, no further analysis is performed. Level 2 offers an opinion on the fairness of real-time financial statements. Level 3 provides an analysis of technical violations of 3rd party contracts (in this case debt covenant compliance is assessed).

Due to the reports being produced on demand (pull) (as opposed to being pushed to the user) this model is less suited to using XBRL-based reporting.

5.4. *Problems limiting use of CA systems*

One of the problems affecting continuous auditing solutions in real-time accounting systems is the varied data formats used. The ability to access and retrieve data from a variety of record sources, including legacy systems, is crucial to the creation of a continuous auditing system. This means that data will be in a variety of formats, with different file types and record systems. It becomes necessary to standardise these data. Unfortunately, this can be a complex and expensive process. Even more problematic is the risk of introducing errors such as duplicate records.

Technologies such as XBRL go a long way in creating a standard reporting format (Srinivas, 2004). Add to this, intelligent technology such as FRAANK (Financial Reporting and Auditing Agent with Net Knowledge) which can convert older reports into XBRL. This can create a way to compare non-XBRL data produced by legacy systems with newer XBRL reports (Kogan et al., 1998).

Until XBRL becomes widely implemented, using data marts to collect and assimilate data is an option. Onions (2003) also suggests adding XCAL, which would create a generic master file layout.

6. Evaluation of models

To evaluate these models one needs to consider at how accuracy and reliability are validated. In this context, *Accuracy* refers to how fraud and error in transactions are detected and how possible material misstatements in financial records are detected. *Reliability* is how confidentiality, integrity and availability of internal controls are examined. Further, these models will also be compared on *Real-time Processing* the *Reporting Method* used and the *Proposed Data Format* (Table 1).

It is apparent that the approaches of the three models differ slightly from each other, however, they all aim to function as close to real-time as possible. Some of the models use different technologies to achieve the same goal. For instance, detecting fraud and error may be accomplished by CAATS, digital agents or expert systems.

In the following section, suggestions will be made on how to draw together the tools and technologies used within these models to create comprehensive future CA systems.

Appendix D

Table 1 – Comparison of three continuous auditing models

	Rezaee et al.	Onions	Woodroof and Searcy
Accuracy (fraud and error) within transactions	Standardised audit tests are built into audit data marts. They run either continuously or at predetermined times. These gather evidence and then generate the relevant reports.	Transactions are checked both at time of entry and later. CAATTS (real-time, not batch). Expert systems (not in "real-time" but running continually).	Rule-based detection by digital agents. Data are analysed by devices integrated into the system.
Reliability of internal control system	CAATS are used. These include Integrated Test Facilities (ITFs) and parallel simulation. ITFs are used to verify correctness and completeness of processing. Parallel simulation tests assess effectiveness of control activities.	Parsing of keystrokes to detect database management utilities. Password control. Operating system's security. Audit logs. Web services verify information (e.g. new supplier's credit history checked).	Adapt and apply SYSTRUST principles. Web-based valuation sites. Must be in the auditor-defined rules for the digital agents.
Real-time	Real-time processing is the aim for this system.	All proposed systems run in parallel with operational systems in real-time.	Real-time reporting is one of the aims of this model. To this end, information must be collected and monitored in real-time.
Reporting method	Web-enabled data delivery of data to auditors' workstations, where reports can be generated (possibly by Generalized Audit Software).	Graded alerts sent through Virtual private networks (VPNs) to audit department/OLSAC. The alerts are graded by gravity (three levels).	Three levels of reporting, alerts are sent to the auditor via email. Level 1: reliability of the system or security of the transmission. Level 2: transactions and processes. Level 3: technical violation of 3rd party agreement. 3rd party and auditor notified by email. Evergreen reports are produced on demand through a web interface – information *pull* approach (as opposed to XBRL reporting this is push reporting method).
Proposed data format	Data mart Data warehouse XBRL	XCAL Data marts	Does not interface with legacy systems.

7. The future of CA technology

To meet the requirements of continuous auditing, any comprehensive CA model would need to address both *internal control testing* and *testing of transactions*. A dual-pronged approach, where both the system (internal controls) and data (transactions) are tested, simultaneously would be the ideal.

7.1. *Internal control issues*

There is a need to collect evidence on the quality and integrity of an electronic system in producing reliable and accurate financial information. Technology must aid in verifying the integrity of data, because the conclusions in auditors' reports must be based on accurate and reliable data in order to be deemed trustworthy (Wessmiller, 2002).

Appendix D

There is also a need to ensure the security of the system. A system which is not secure is not reliable. Ensuring security would involve examining internal controls. If the system is not reliable, the results from that system may not be viewed as trustworthy. Woodroof and Searcy (2001) suggest SYSTRUST (or a CA derivative of SYSTRUST). COBIT Guidelines in conjunction with ISO 17799 could also be used. COBIT could address internal control related issues (The IT Governance Institute, 2005). ISO 17799 would aid in addressing information security issues (ISO/IEC 17799, 2005). Thus, a number of best practices and/or standards exist to address the security issues.

Rezaee et al. (2002) mention Concurrent Audit Techniques for testing effectiveness of a client's internal controls. Concurrent Audit Techniques include SCARF (Systems Control and Review Facility) and the snapshot approach, where SCARF functions as an exception reporting system. It captures transactions meeting certain criteria (defined by the auditor) by using Embedded Audit Modules. The captured transactions are set aside for later review by an auditor. Embedded Audit Modules and the SCARF approach could be used to create alerts regarding the status of internal control systems by checking if controls are implemented.

7.2. *Transactions*

Processing of transactions should occur in several stages. Various technologies help throughout these stages. Firstly, transactions from a variety of sources are extracted. Not all records or fields may be required, digital agents and stored database procedures could be used to pull out only the necessary data. The creation of data marts and data warehouses may be desirable, a capable Database Management System (DBMS) would be required.

Once data have been collected and transformed, the transactions need to be assessed. Transactions are individually assessed for integrity (errors and fraud) and validity (business rules). CAATTS can be made to run as close to real-time as possible, while the data are flowing through the application system. Both analytical procedures and substantive testing should be applied to look for fraud and error. Common IT-based fraud schemes often involve the billing system, payroll system and check tampering. These schemes often need to be identified at the transaction data level, as they can depend on groups of transactions within the system. Examples include ghost vendors, ghost employees and exploiting voids and returns (Taylor, 2005).

Often a Database Management System (DBMS) forms an important part of a system. An example of a commonly used DBMS is Oracle. Oracle is a DBMS which allows "triggers" to perform tasks when certain criteria are met. Triggers are useful for creating logs for system events (Finnigan, 2003). Triggers in a database can be used in the same way as Data Query Modules (DQMs). DQMs are macros or programs built using audit software, they perform queries to answer a specific question posed by the auditor. For example, DQMs could be used to look for fraudulent travel allowance claims of employees. Employee swipe card data could be compared to dates on tour and travel reports. If the employee's card was swiped, and they were at the office, they are most likely claiming travel allowance for extra days (Dalal, 2000). If the entry of a new travel claim triggered the execution of the relevant DQM, an instant audit would occur.

At this stage, alerts could be produced. For example control agents may be used to alert auditors if transaction values change too much from the norm. The relevant transaction data need to be collected for future forensic analysis – possibly by moving the data to a secured partition or dedicated audit server. This may be achieved using FTP and tape or other large-capacity storage devices. Digital agents then examine transactions and select those that should be set aside for later analysis. CIS (Continuous and Intermittent Simulation) could also be used for deciding which transactions require more examination.

The data may then need to be standardised. This may be done either on the audit server or in the source application, depending on the cost of processing. For example, the cost of processing on mainframes is more expensive. The data can then be aggregated in data marts or data mines. Data mines are expensive and normally only larger organisations can afford them. Data marts are often used by smaller organisations, or in larger organisations for one specific focus area, for example, Human Resources, Accounting data, etc. (Rezaee et al., 2001). Smaller organisations could also make use of XCAL, as suggested by Onions (2003).

Stored data may then be checked for groups of transactions and the cumulative effects of a series of transactions. Expert systems and digital agents may be very useful for this purpose. Analytical procedures could also be used to create "norms" which can be used as a benchmark. The results of these tests are then used to create reports and alerts, which are sent to auditors by encrypted email. The alerts may also be sent via VPNs. A grading system for alerts, showing the possible impact of the anomaly, may be important to the auditors.

It may also be necessary to be in contact with an outside auditing bureau for verification and validation. For example the Online Systems Audit Centre (Onions, 2003). The Online Systems Audit Centre is a group of auditing professionals, which monitor and investigate alerts online. VPNs can be used for this purpose. Web-enabled agents like FRAANK, and Web Services may also provide useful, secure ways to communicate (Kogan et al., 1998; Murthy and Groomer, 2004).

8. Conclusion

Within real-time accounting systems, real-time assurances are not only desirable, but are possible. Technologies which enable the provision of real-time assurances are becoming commonplace. This includes technologies which test internal controls and those related to testing transactions. Many of these technologies are not new, for example CAATTS, including GAS, EAMs and ITFs, which are being applied in new ways to achieve continuous auditing. Some innovative technologies, such as AI technologies allow every transaction to be inspected, instead of just a sample. These available technologies need to be brought together in a way which makes full use of each of them.

Models have been suggested for this purpose, however, most are only conceptual. These models can be adapted and

adjusted in order to provide the auditor with the reliable and accurate results he or she desires. A possible reason for the lack of comprehensive continuous audit models may be the result of the problems related to the variety of data formats which exist and the availability of audit data. Technologies such as XBRL contribute to solving the problem, but further enhancements are definitely envisaged.

A comparison of the three most prominent continuous auditing models is tabulated. The models are compared according to a set of criteria. These include: how accuracy and reliability are evaluated, what the reporting method is, and how close to real-time the model functions, and the proposed data format. These findings highlight the core aspects of the three models and can be used as a foundation on which to build future continuous auditing solutions.

REFERENCES

Alles M, Kogan A, Vasarhelyi M. Real time reporting and assurance: has its time come? Available from: http://raw.rutgers.edu/continuousauditing/Real_Time_Reporting_-_ICFAI1.doc; 2004 [retrieved 12.05.2005]

American Institute of Certified Public Accountants (AICPA). Amendment to statement on auditing standards no. 31, evidential matter: SAS 80; 1996.

Bierstaker JL, Burnaby P, Thibodeau J. The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. Managerial Auditing Journal 2001;16(3):159–64.

CICA/AICPA. Continuous auditing: research report. Canadian Institute of Chartered Accountants; 1999.

Dalal C. Advanced use of audit software in audit and fraud detection – audit software: an indispensible tool in the new millennium. Ineternal Auditors 2000;3(February 1).

Finnigan P. Introduction to simple oracle auditing. Available from: http://www.securityfocus.com/print/infocus/1689; 2003 [retrieved 10.04.2006].

Flowerday S, von Solms R. Real-time information integrity = system integrity + data integrity + continuous assurances. Computers and Security 2005;24:604–13.

Helms GL, Mancino J. Wave good-bye to the paper trail. Electronic auditor. Available from: http://www.aicpa.org/pubs/jofa/apr98/helms.htm; 1998 [retrieved 7.03.2005].

Helms GL, Mancino JM. The CPA & the computer: information technology issues for the attest, audit, and assurance services functions. Available from: http://www.nysscpa.org/cpajournal/1999/0599/departments/cpac.html; 1999 [retrieved 3.05.2005].

ISO/IEC 17799. Information technology – security techniques – code of practice for information security management. International Organization for Standards. Available from: http://www.iso.org/iso/en/ISOOnline.frontpage; 2005.

Kogan A, Nelson K, Srivastava R, Vasarhelyi M, Bovee M. Design and applications of an intelligent financial reporting and auditing agent with net knowledge. Available from: https://kuscholarworks.ku.edu/dspace/bitstream/1808/141/1/srivastava.pdf; 1998 [retrieved 10.05.2005].

Murthy US, Groomer SM. A continuous auditing web services model for xml-based accounting systems. International Journal of Accounting Information Systems 2004;5:139–63.

Onions RL. Towards a paradigm for continuous auditing. Available from: http://www.auditsoftware.net/community/how/run/tools/Towards%20a%20Paradigm%20for%20continuous%20Auditin1.doc; 2003 [retrieved 1.04.2005].

Pinkster R. XBRL awareness in auditing: a sleeping giant? Managerial Auditing Journal 2003;18(9):732–6.

Rezaee Z, Elam R, Sharbatoghlie A. Continuous auditing: the audit of the future. Managerial Auditing Journal 2001;13(3):150–8.

Rezaee Z, Sharbatoghlie A, Elam R, McMickle P. Continuous auditing: building automated auditing capacity. Auditing: A Journal of Practice and Theory 2002;21(1):147–63.

South African Institute of Chartered Accountants. SAICA handbook – auditing. 2003/2004 ed., vol. 2; 2003.

Srinivas S. Road map to XBRL adoption as a new reporting model. Information Systems Control Journal 2004;1.

Taylor P. The perils of systems-based fraud. IT Audit 2005;8(January 15).

The IT Governance Institute. (COBIT) Control objectives for information and related technology. 4th ed. USA: The IT Governance Institute; 2005.

Vasarhelyi MA. Concepts in continuous assurance. Available from: http://raw.rutgers.edu/continuousauditing/conceptsincontinuousassurance13final.doc; 2002 [retrieved March, 2005].

Varsarhelyi MA, Halper FB. The continuous audit of online systems. Auditing: A Journal of Practice and Theory 1991;10(1).

Wessmiller R. Facing the data integrity challenge. Available from: http://www.theiia.org/itaudit/index.cfm?fuseaction=print&;fid=440; 2002 [retrieved 20.04.2005].

Woodroof J, Searcy D. Continuous audit: model development and implementation within a debt covenant compliance domain. International Journal of Accounting Information Systems 2001;2:169–91.

Stephen Flowerday is currently a final year full-time doctoral student at the Nelson Mandela Metropolitan University in South Africa. His research focus is on providing real-time assurances for information integrity. This is within the domain of corporate governance and information security management. In addition to his studies he lectures part-time and before entering the academic field he had a successful career in management consulting.

Adrian Blundell is presently completing a full-time Master's degree in Information Technology at the Nelson Mandela Metropolitan University in Port Elizabeth, South Africa. He is researching the roles of various technologies within continuous auditing systems. His qualifications include a National Diploma IT from the Port Elizabeth Technikon and a B. Tech IT from Nelson Mandela Metropolitan University.

Professor Rossouw von Solms is the Director of the Institute for ICT Advancement at the Nelson Mandela Metropolitan University in South Africa. He holds a PhD from the Johannesburg University. He has been a member of the International Federation for Information Processing (IFIP) TC 11 committee since 1995. He is a founder member of the Technikon Computer Lecturer's Association (TECLA) and is an executive member ever since. He is also a vice-president of the South African Institute for Computer Science and Information Technology (SAICSIT). He has published extensively in international journals and presented numerous papers at national and international conferences in the field of Information Security Management.