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

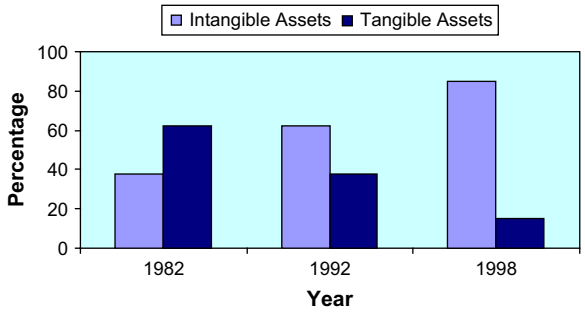

Figure 1 Percentage of company market value related to tangible and intangible assets (Brookings Institute & Baruch Lev's Analysis).

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.

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:

$$\begin{aligned}&\text{Expected Value of Risk}\\&\quad=\text{Estimated Loss from Specific Risk }(\$)\\&\qquad\times\text{Likelihood of Loss }(\%)\end{aligned}$$

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

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,

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.

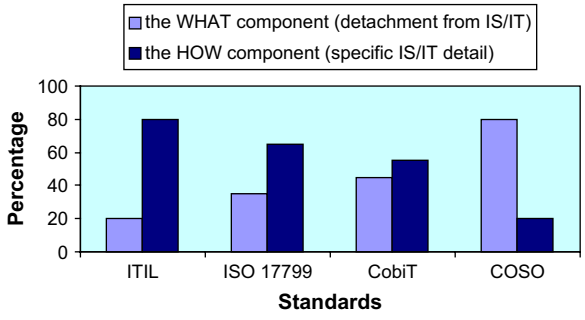

Figure 2 A general guide that illustrates the standard's tendency towards IS/IT or business.

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.

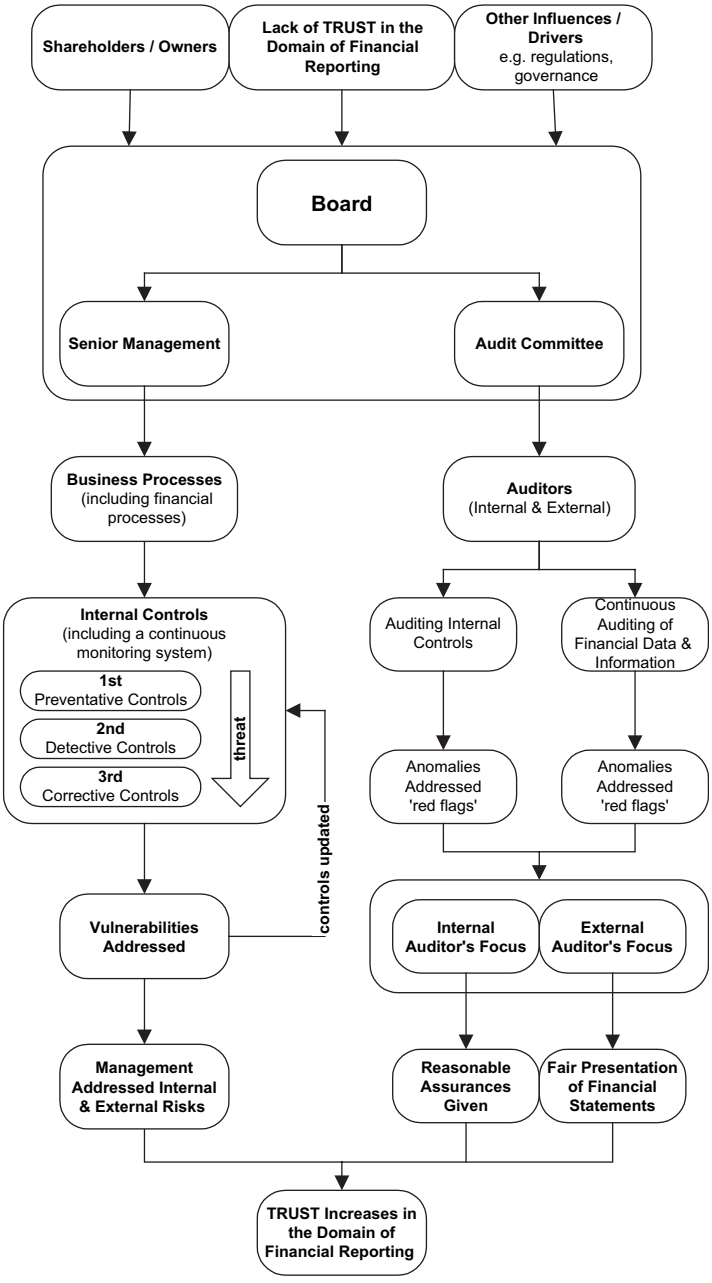

Figure 3 High-level flowchart illustrating the management and audit processes.

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.