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.

Knowledge is power: protecting privacy

Stephen Hinde

For also knowledge itself is power. Thus wrote Francis Bacon in Meditationes Sacrae (1597). This became shortened in proverb to Knowledge is power, which is the title and the theme of Richard Thomas,the UK Information Commissioner, in the 21st Annual Report to the UK Parliament (2004-2005).

The Commissioner's Office is an independent public body which has a statutory duty to promote access to official information (the Freedom of Information Act 2000) and protect personal information (the Data Protection Act 1998).

Knowledge is power underlines the fundamental importance of both freedom of information and data protection at the beginning of the 21st century. According to the Commissioner it also highlights the common threads between the two. They differ, in that freedom of information brings official information into the open, while data protection safeguards personal information. But they are also similar, in that both are focused on good practice in handling information and both create important access rights to it.

Freedom of information

Freedom of information brings knowledge to the people - who must be the ultimate custodian of power in any genuine democracy. It allows people to see what government, at every level, is doing on their behalf and with their money. Transparency is crucial to accountability. The principles and rights available under freedom of information laws provide a powerful reminder that governments serve the people, and not vice versa.

Data protection

In parallel, data protection stops too much information about our personal lives ending up in the hands of government, commercial or voluntary organisations. It is essential to restrain the power which comes with too much knowledge about our private lives. Data protection erects barriers in the way of a surveillance society. It is needed to ensure that our personal information is used for intended purposes, is accurate, is kept up to date and is kept secure.

The threats to personal data are threefold:

- By government (normal government and in the guise of fighting terrorism and organised crime);
- By business for marketing purposes, credit vetting etc; and
- By criminals for theft, beit straight forward theft using another's financial information or the more serious identity theft.

The Commissioner at the launch of his Annual Report spoke of the black market in personal data. Such is his concern that