THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 6 | Number 2 Article 4

2011

Developing a Forensic Continuous Audit Model

Grover S. Kearns
University of South Florida, St. Petersburg

Katherine J. Barker
University of South Florida, St. Petersburg

Stephen P. Danese
University of South Florida, St. Petersburg

Recommended Citation
Kearns, Grover S.; Barker, Katherine J.; and Danese, Stephen P. (2011) "Developing a Forensic Continuous Audit Model," *Journal of Digital Forensics, Security and Law*: Vol. 6 : No. 2 , Article 4.
DOI: https://doi.org/10.15394/jdfsl.2011.1094
Available at: https://commons.erau.edu/jdfsl/vol6/iss2/4

DEVELOPING A FORENSIC CONTINUOUS AUDIT MODEL

Grover S. Kearns, Ph.D., CPA, CFE
Gregory, Sharer & Stuart Term Professor in Forensic Accounting
gkearns@usfsp.edu

Katherine J. Barker, CPA, CFE
Assistant Professor in Accounting
barker@usfsp.edu

Stephen P. Danese
Instructor in Accounting
danese@usfsp.edu

College of Business
140 7th Avenue South
University of South Florida St. Petersburg
St. Petersburg, FL 33701

ABSTRACT

Despite increased attention to internal controls and risk assessment, traditional audit approaches do not seem to be highly effective in uncovering the majority of frauds. Less than 20 percent of all occupational frauds are uncovered by auditors. Forensic accounting has recognized the need for automated approaches to fraud analysis yet research has not examined the benefits of forensic continuous auditing as a method to detect and deter corporate fraud. The purpose of this paper is to show how such an approach is possible. A model is presented that supports the acceptance of forensic continuous auditing by auditors and management as an effective tool to support the audit function, meet management's regulatory objectives, and to combat fraud. An approach to developing such a system is presented.

1. INTRODUCTION

Over the past decade, businesses have faced increased regulatory oversight and reporting requirements combined with global competition and increased costs of raw materials and labor. As a result, management seeks an efficient but effective approach to governance which satisfies compliance requirements but also protects the organization from fraud at an affordable cost.

With organizations routinely processing terabytes of information daily achieving important audit objectives has become a daunting task. Traditional audit

approaches and sampling methods cannot be expected to uncover the majority of transactional errors or occupational fraud (Wells, 2011; Oringel and Aldhizer, 2009). Technology offers opportunities to detect and deter fraud more efficiently and effectively. Statement on Audit Standards No. 99 (SAS 99), *Consideration of Fraud in a Financial Statement Audit*, codifies many fraud detection procedures and encourages their use by auditors to detect client fraud risk and identify transactions to be tested (AICPA 2002, AU 316.52, AU 316.61; Lanza and Gilbert, 2007). Technological skills, however, often exceed the competency of auditors causing them to resort to less effective manual approaches.

The regulation that has had the most profound impact on management and auditors in the past decade, the Sarbanes-Oxley Act of 2002 (SOX02), requires that CEOs and CFOs assess and attest to the effectiveness of the organization's internal control structure. It also imposes increased penalties for financial statement fraud. Both SOX02 and SAS 99 encourage management and external auditors to employ technological approaches and embedded audit modules to audit financial transactions and internal controls (Roth and Espersen, 2003). Forensic continuous auditing (FCA) will result in a stronger internal control environment by detecting a greater percent of transactional errors and anomalies that might indicate fraud or misuse. The low percentage of frauds currently uncovered by external and internal auditors affirms the ineffectiveness of traditional techniques.

SOX02 Section 409 accelerates the SEC filings for Form 10-Q and annual report Form 10-K. The new rules will eventually require public companies to file annual reports within sixty days of their year-end and quarterly reports within thirty-five days of the end of the quarter. The FTC's red flag rules, effective December 31, 2010 for financial institutions and certain other firms under FTC jurisdiction including CPA firms, require companies to check for and report specific violations. These rules are expected to increase compliance costs. Automating the audit process will enhance the company's ability to comply with these reporting requirements and lower overall governance costs. Although increased regulatory pressure mandates more attention to internal controls, these pressures could actually increase fraud opportunities by overwhelming management and auditors with reporting requirements.

Despite increased attention to internal controls and risk assessment, traditional audit approaches lack effectiveness in uncovering occupational fraud. In its *2010 Report to the Nations*, the Association of Certified Fraud Examiners (ACFE) noted that most of the frauds were uncovered by anonymous tips and less than 20 percent are uncovered by either internal or external auditors. This is partly because external auditors focus on the organization's financial statements only once a year and most auditing concentrates on small sample sets of selected transactions over fixed periods of time. A more effective approach would be to audit all or a large part of the transactions continuously.

Continuous auditing, which has been the focus of much research and has notable successful implementations (Alles and Vasarhelyi, 2008), still eludes many companies (Alles et al., 2008). The major barriers are technical – the lack of embedded audit modules (EAMs) and auditor's lack of the requisite technical skills (Li et al., 2007). Once operable, however, continuous auditing systems require less technical expertise and offer auditors a wealth of information that can increase audit quality while reducing the overall workload.

Forensic accountants have recognized the need for automated approaches to fraud analysis yet research has not examined the benefits of continuous auditing as a method to detect and deter corporate fraud. The purpose of this paper is to show how such an approach is possible. Contributions are twofold. First, cogent arguments are presented, in the form of five propositions that support the necessity for a system of forensic continuous auditing. Second, the paper presents an approach to forensic continuous auditing that is scalable and can be phased-in to accommodate the needs of management, auditing and information technology.

2. DEVELOPING THE FORENSIC CONTINUOUS AUDIT MODEL

2.1 Impact of Regulation

Management concerns about fraud have been heightened in the post-SOX02 environment due to increased penalties for financial statement fraud and governance requirements for a costly internal control framework. Requirements for auditors have increased dramatically and are costly. SOX02 Sec. 404 requires management to evaluate and attest to the internal control structure within ninety days of the audit report date. Increased compliance is costly and increases audit fees. For example, SOX02 Sec. 404, which requires management to evaluate and attest to the internal control structure within ninety days of the audit report date, os estimated to have cost Fortune 100 companies about $7.8 million in 2005 of which audit fees were $1.9 million (Nondorf et al. , 2011).

Public Company Accounting Oversight Board (PCAOB) Auditing Statement 2, *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*, states that it is management's responsibility to design and implement a program of controls to prevent, detect and deter fraud.

According to the ACFE, estimated fraud losses in the United States for 2008 were $994 billion. The highly publicized frauds of the past decade have led to increased emphasis on internal controls. Adoption of the *Committee of Sponsoring Organizations* (COSO) framework and Statement on Auditing Standard No. 78, *Consideration of Internal Control in a Financial Statement Audit*, place greater demands on external auditors. The more detailed information technology (IT) controls, such as those found in the *Control Objectives for Information Technology* (COBIT) framework, have made IT audits standard for larger companies. Lack of technical expertise to conduct such audits has caused many

audit firms to seek out and depend upon more expensive third-party support.

In SAS 99, the AICPA basically mirrored the tenets of SOX02 and increased the auditor's due diligence responsibility for recognition of fraud. It also recommended extended use of technology for substantive testing and audit of controls. Auditors recognize that traditional audit practices that rely heavily on sampling small sets of transactions on a limited basis are not sufficient for evaluating internal controls or for detecting and deterring fraud. Also, financial audits that are based primarily on substantive testing and neglect detailed analysis of transactions or auditing through the computer cannot provide high levels of assurance.

2.2 Auditing for Fraud

Traditional audit techniques are not sufficient and do not provide continuous assurance. Nor are they likely to uncover the most risky frauds – those perpetrated by managers who can override controls and alter ledger and journal entries. In order to audit *through* the computer, a process is necessary that allows for testing of a significant number of transactions on a real-time basis and throughout the year rather than brief discrete intervals. The process should focus on areas of high risk, areas of concern by key stakeholders, and risks that are significant – those that may be unlikely but where an adverse incident could threaten the life of the enterprise. Through control frameworks such as COSO and COBIT, companies monitor and assess activities to detect incidents of errors, misuse and fraud and respond in a timely manner.

To determine the likelihood that financial statements contain material misstatements, auditors conduct tests of transactions and substantive tests. Tests of transactions determine whether erroneous or falsified data have been processed. Substantive tests examine balances such as accounts receivable and accounts payable, inventories, liabilities and depreciation to provide assurance that financial statements are free from material misstatements (Rezaee et. al, 2001). Normally, if tests of transactions do not reveal irregularities then less reliance is required on substantive testing. However, if tests of transactions reveal abnormalities then substantive testing must be expanded. In a continuous auditing environment, tests of transactions is an ongoing process and evidence is collected on a larger set of transactions and over a wider time-frame that with traditional methods. This lessens the need for substantive testing and reduces the role of the external auditors resulting in savings for the client firm.

As a result of new regulatory requirements for compliance and emphasis on IT governance, auditors with forensic IT skills have been in increased demand (Hoffman, 2004). Because IT control deficiencies lead to accounting and financial reporting errors (Alaali, Grant, and Miller, 2008), it is important that auditors be able to identify IT problems that affect financial reporting, evaluate the extent and nature of the problems and be familiar with steps to correct these weaknesses (Grant et al., 2008). The Forensic Continuous Audit Model is shown in Figure 1.

The first requirement is continuous auditing.

3. CONTINUOUS AUDITING

3.1 Advantages of Continuous Auditing

According to the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) "A continuous audit is a methodology that enables independent auditors to provide written assurance on a subject matter, for which an entity's management is responsible, using a series of auditors' reports issued virtually simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter." (AICPA/CICA Research Study on Continuous Auditing, 1999).

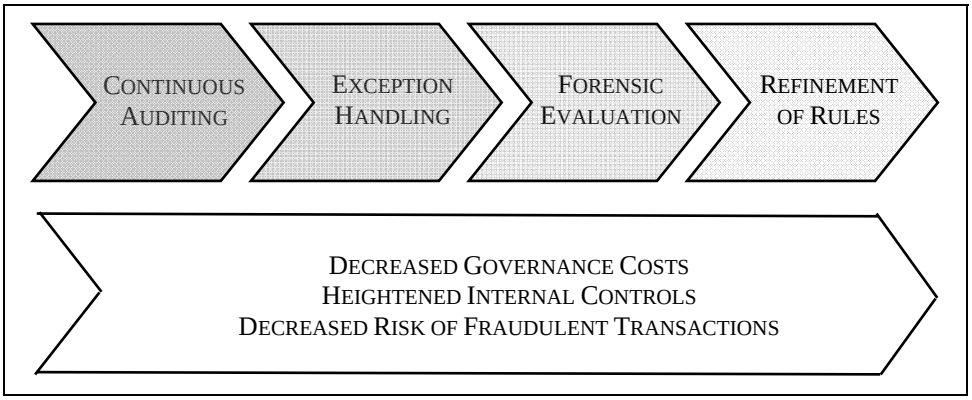


Figure 1: Forensic Continuous Audit Model

Because auditors often lack technological skills, a large percentage of companies rely primarily upon manual methods to evaluate internal controls. Consequently, these companies cannot determine how effective their control processes are on a daily basis despite large investments in governance (KPMG, 2010). In a 2009 survey by the Institute of Internal Auditors, only 32 percent of 305 companies reported that they performed continuous auditing. By providing for automatic analysis of transactions, continuous auditing would relieve the auditors of the burdensome strain and allow greater focus on the analysis of suspicious transactions.

3.2 Impact on Auditors and Governance

Continuous auditing offers several advantages for auditors. Because it tests more transactions over a wider time-frame, it provides more comprehensive and timely assurance. Also, it is scalable allowing the magnitude and timing of tests to be performed based upon the assessed risk of the targeted transactions. It can reduce the amount of substantive testing performed during financial audits and allow greater focus on more important investigative matters. It can reduce audit risk and

increase management confidence in financial reports. It supports compliance reporting and reduces both errors and fraud. While continuous auditing assumes that all transactions are monitored in real-time, judicious application of the cost/benefit rule would schedule tests based upon the likelihood and severity of the risk. Performing the analytical procedures on a routine basis would lessen the work of the independent auditors and reduce their time on-site thus avoiding costly tests and unnecessary distractions during the workday.

Tests of transactions using analytical procedures plus confirmation of account balances and events are the most common work product of financial audits. Confirmations may be either positive or negative. The negative confirmation is expected to be responded to only if the balance is not accurate. Research shows, however, that negative confirmations may not signify correctness as recipients may ignore them or they may be lost by mishandling (Aldhizer and Cashell, 2006; Caster and Sriram, 1996). When limited to small sample sets, tests of transactions may not be representative and cannot be expected to detect a large percent of errors or fraudulent activities. Given the increased transaction processing for most firms and increased regulatory pressures, the traditional approaches appear inadequate and require increased substantive testing.

KPMG's 2008 publication, *Continuous Auditing/Continuous Monitoring: Using Technology to Drive Value by Managing Risk and Improving Performance*, comments that: "As business risks of all kinds continue to proliferate, management and internal audit departments are actively seeking new ways to quickly gain access to valuable information to manage risk and improve performance. Such efforts increasingly include continuous auditing and continuous monitoring of organizational processes, systems, and controls."

3.3 Cost Savings

Continuous auditing can result in substantial savings by reducing the amount of external auditor fees (Hermanson et al., 2006). Thus, it reduces overall governance costs while reducing the opportunity for errors or fraud. Measuring cost savings from CA is made difficult by the number of applications to which it is applied, the extent of testing and the frequency of testing. Thus, one company could be performing more extensive testing than others that claim to engage in CA. Siemens has claimed a substantial return from implementing CA in an ERP environment (Alles et al., 2006). They added both detective and preventive controls to an existing SAP system and use manual procedures to handle exception alerts. Detective controls allow auditors to uncover incidents of internal control violations. Preventive controls assist to insure internal controls are followed.

Continuous auditing is also "more timely, comprehensive, accurate and less costly" (Alles et al., 2006, p. 212). It can also free up time so internal auditors can pursue other value-added services (Oringel et al., 2009). These cost savings are likely to lure more companies into the CA waters.

3.4 Forensic Continuous Auditing

FCA differs in the respect that more focus is placed upon the evaluation of sophisticated audit rules and examination of trends and anomalies that may reflect underlying errors or fraudulent commissions. FCA places more emphasis on the analysis of sensitive data sets and less emphasis on transactions for which detection risk is low. It also provides for a greater range of analysis and emphasizes improvement of the audit rules over time.

Regulatory standards encourage the use of computer assisted audit tools and techniques (CAATs) for accessing and analyzing data files and suggest that risk assessment reflect the client IT standards (AICPA 2001, 2006). Recent research, however, indicates that only a minority of firms use CAATs for substantive testing because of the high level of complexity (Janvrin et al., 2009). Continuous auditing can provide much of the substantive testing in a routine manner and allow auditors to concentrate on the forensic analysis of data.

3.5 Developing an Approach to Forensic Continuous Auditing

There are various approaches to continuous auditing. The embedded audit module (EAM) approach depends upon audit specific software that resides in the targeted application (Alles, 2002). It allows auditors to determine which transactions are to be tested and at what frequency. Results are collected and reported real-time. Enterprise resource planning (ERP) systems often contain EAM functionality (Groomer and Murthy, 1989). Surveys show, however, that companies that use enterprise resource planning (ERP) systems often do not activate the EAM because of the significant resource requirements which can slow overall processing dramatically (Kuhn and Sutton, 2010; Debreceny et al., 2005).

The technical nature of EAMs require that auditors acquire a higher levels of technical skills to implement these tools effectively and may hamper their adoption (Debreceny et al., 2005). Some researchers state that auditors cannot effectively administer continuous auditing because of low technical proficiency and inability to communicate with IT personnel (Li et al., 2007).

An alternative approach is the monitoring control layer (MCL) which uses an external software module linked to the target applications and databases (Vasarhelyi et al., 2004).

Creating a virtual environment allows the EAM or MCL to be used outside the production version of the application and avoid system performance problems. System ghosting creates a copy of an entire system on separate hardware and eliminates any risk associated with processing live transactions. Table 1 presents the steps for developing a FCA system.

Table 1: Developing a Forensic Continuous Audit System

1. Examine internal controls for adequacy to mitigate risks. 2. Determine which risks are most likely or could cause the most harm to the organization. These risks should be continuously audited. 3. Examine each risk to determine the appropriate audit rules to be applied. 4. Examine each risk to determine the appropriate number of transactions to be tested – this will vary depending upon perceived risk and management objectives. 5. Examine each risk to determine the appropriate frequency of auditing – continuously, hourly, daily, weekly etc. 6. Identify target applications and databases for the associated transactions and events. 7. Establish a protocol for reviewing and handling the selected transactions. 8. Build the link between the CAAT and the data file to automate the continuous audit cycle. Create a Virtual Environment on the audit server. 9. Maintain an audit trail of the selected transactions and examine trends and anomalies. 10. Refine the audit rules making modifications based on experience. 11. Report results to management, the audit committee and external auditors. 12. Set alarms for suspicious transactions or events that require immediate action.

In the FCA Model, the second requirement is exception handling which applies the audit rules in order to uncover errors and suspicious transactions.

4. EXCEPTION HANDLING

4.1 Handling of Selected Transactions

Exception handling is critical to the efficacy of continuous auditing. By performing a large number of tests over a much higher percentage of transactions, continuous auditing expands the testing of details to a large percentage of the overall data and can reduce reliance upon analytical procedures (Alles et al., 2008). It will also result in a large number of selected transactions that have failed the audit tests. FCA takes the process one important step further: it adds analytical tools to examine the selected transactions for possible errors or acts of fraud.

Transactions that trigger exceptions or alarms must be responded to in a timely manner by qualified individuals with forensic knowledge and skills. Exceptions could be handled by internal auditing. Hermanson et al. (2006) suggests that software be coded to categorize incidents (selected transactions or events) into three categories: errors, misuse, and fraud. By responding to errors immediately, the source department may be able to take corrective action that eliminates future errors. System misuse could lead to increased employee training and awareness. It could also indicate the need for adjusting policies.

Selected transactions that require the most scrutiny and careful response are those that indicate the possibility of fraud. Protocols for handling these special events should be established in order to facilitate a quick and consistent response. In any event, managers should be alerted and action taken to prevent or isolate any further occurrence of the event. As Smith (2005) points out, as the time lag increases between the suspicion of fraud and the recovery of forensic data, evidence becomes less valuable. Larger companies may have an incidence response team. If so, they will probably require an analysis of the situation that could be performed by the internal audit group. Since SOX02, internal audit has reported to the audit committee which is comprised of outside board members. This has lessened managerial pressure that might have compromised the past effectiveness of the internal audit group. Also, external auditors, an independent third body, examine the work of internal auditors that becomes part of the final external audit. Internal auditors should play an important role in fraud investigation. In public companies, internal auditors must now report directly to the audit committee which is composed of outside board members. Also, PCAOB 5 proscribes the use of internal auditors in the use of substantive testing and other parts of the public audit and the internal audit function is perceived as maintaining a professional and objective stance in regards to the audit reports. Using the FCA process, internal auditors can examine data sets to uncover and document fraudulent commissions. The FCA process may be the first line of defense in proactively identifying possible fraud.

Auditors may also play an investigative role in the development and maintenance of forensic evidence. This might require the auditor to perform read-only searches, preserve time-stamps, secure data and maintain a proper chain of custody (Smith, 2005).

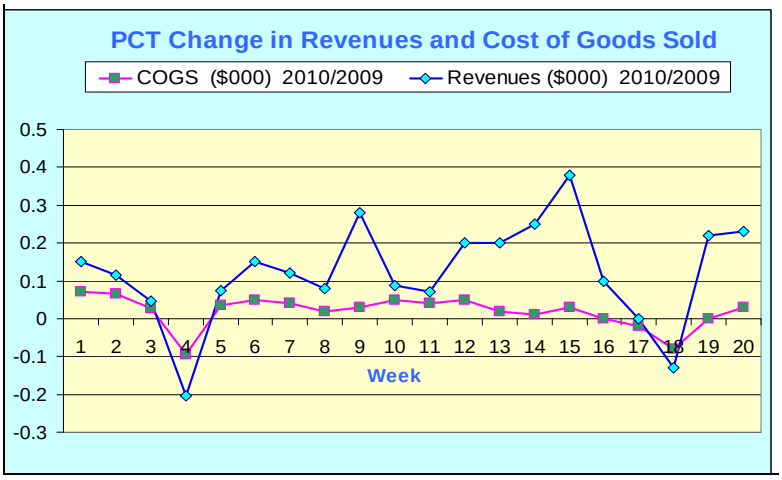


Figure 2: Trending Revenues with Cost of Goods Sold

4.2 Audit Rules

Regulators and the public expect auditors to uncover fraud. Research, however, does not support the ability of either external or internal auditors to uncover significant amounts of fraud (Albrecht et al., 2001). Thus, auditors must be trained to seek out specific types of fraud when analyzing the selected transactions. Special attention should be given to revenue manipulation and income-increasing manipulation because these are the most frequently occurring items in financial statement fraud (Johnson and Ireland, 2007). Transactions that fail the audit rules or highlight anomalies would be selected for forensic evaluation by internal auditors. For example, in Figure 2, the relationship between revenues and cost-of-goods sold is tracked over time. Revenues may be expected to vary but the relationship between revenues and cost-of-goods should exhibit a low variance and remain fairly smooth. In Figure 2, anomalies are readily apparent. These discrepancies require investigation and could reveal a fraudulent misstatement of revenues. The third requirement of the FCA Model is forensic evaluation of the selected transactions to determine what actions should be taken.

5. FORENSIC EVALUATION

Selected transactions might also uncover control weaknesses. For example, monitoring of access rights might identify instances of employee attempting to access unauthorized files or incompatible sets of files. The event would allow supervisors to take immediate action and correct the problem and modify the control.

Continuous auditing and monitoring can be expected to increase the likelihood that all fraud, including financial statement fraud, is reduced or detected in a timely manner. A large percentage of transactions are investigated and some results are presented in a graphical format. Transactions that fail audit rules would be written to a selected transactions file. Forensic evaluation using extended analytical procedures applied to the selected transactions allows proper and timely scrutiny. The forensic evaluation should examine the relationships between financial data within a period and over periods to detect anomalies that require investigation.

Financial statement fraud can have a devastating impact on a firm's stock price causing shares to drop as much as 1,000 times the fraud amount (Albrecht et al., 2001). Financial statement fraud in the United States accounted for 68 percent of reported fraud losses in 2009 (ACFE, 2010). Because executive management has the ability to override controls, this type of fraud is more difficult to detect. By examining relationships, such as the ones presented in Figure 2, auditors can ascertain and quickly examine deviations in revenues. Most financial fraud involves revenue manipulation. Being able to question anomalies faster will place executive management on the alert and help to deter such actions in a proactive manner.

FCA systems could monitor 100 percent of an organization's financial transactions and business activities in real-time. Automating the analysis and testing reduces the cost of SOX02 compliance and reduces the risk of loss beyond what could be expected of periodic testing of small transaction sets.

5.1 Analytical Tools

Although many firms have adopted ERP solutions and have access to embedded audit routines, there are valid arguments for examining a modified approach to FCA. Research has shown limited support for the use of embedded audit modules in ERP systems (Debreceny et. al, 2005). Firms may have multiple ERP systems and each would require auditors to master the internal EAM. EAMs that operate internally can cause significant reductions in performance. An alternative is to use generalized audit software and apply established audit rules to transaction files in order to uncover erroneous or fraudulent transactions.

Audit Command Language (ACL) and Interactive Data Extraction and Analysis (IDEA) are well known audit software that can be used for developing CAATs. Both can be learned without extensive training and have a high level of vendor support. ACL, for example, offers the ability to conduct continuous auditing over several ERP systems and other applications. In addition to supporting a large number of analytical functions these CAATs are capable of extracting data from a large number of file formats. Using ACL analytics such as Benford Analysis, one investigative audit by Forensic Strategic Solutions uncovered more than $70 million of fraudulent expenditures (ACL, 2011). Events such as these could be detected routinely using established fraud audit criteria to test transactions and controls. Controls could allow selected transactions to be further inspected using other computer tools that support forensic analysis. For example, Benford analysis uses a *z*-statistic to measure the probability that a group of data falls outside the expected distribution. For certain data sets, transactions for which the first digit was outside a *z*-statistic of 2.0 could be triggered for further examination. The trigger points could be adjusted based upon experience. Correlation and time-series analysis can also be used to detect errors and fraud in the selected transactions (Nigrini, 2006). The final stage of the FCA Model is refinement of the rules.

6. REFINEMENT OF RULES

6.1 Designing Audit Rules

Examples of possible audit tests are shown in Table 2. Such tests are commonly performed manually on smaller sets of transactions and at distinct time intervals. The audit rules can test for errors, fraud, and the strength and presence of internal controls while also performing some substantive tests. Results can be used to create compliance reports. Refining the rules will require the judgment of experienced internal auditors based upon the performance of the fraud audit model. Rules can be modified based upon perceived risks and management

objectives. Audit rules drive the analysis of transactions and events. These analytical criteria are created to flag transactions that violate policy or could indicate a fraudulent act. If the criteria are too stringent a large number of alarms (called alarm flooding) will be produced. To prevent the enormous number of false positives audit rules must be properly calibrated (Kuhn and Sutton, 2010; Alles et al., 2008).

If too loosely set the tests could fail to detect a large percentage of erroneous and fraudulent transactions. A major benefit of such a process is that the audit rules can be expanded and periodically evaluated for efficacy and adjusted based upon performance. Over time, experience-based adjustment of the audit rules can make them more efficient and effective. Fraud audit tests should be designed around objectives.

6.2 Forensic Analysis of Selected Transactions

Selected transactions can provide information to proactively detect impending frauds. By examining trends in certain data series, anomalies can be inspected for possible defalcations. Chen and Sennetti (2005) demonstrated seventeen financial and non-financial variables useful in predicting fraud. Most important were, relative to sales, lower research and development costs, lower marketing costs, and lower changes in free cash flows.

Special attention should be paid to financial statement fraud which is the most costly and often requires an override of internal controls. Financial statement fraud and earnings mismanagement can be detected through the judicious application of a set of quantitative and qualitative red flags (Grove and Cook, 2004). An overstatement of revenues would be a possible indicator (Johnson and Ireland, 2007).

Table 2: Examples of Fraud Audit Tests

Fraud Objective	Fraud Flag	Fraud Audit Tests
Fraudulent vendors	Vendor address P.O box, Vendor address matches employee address, Multiple vendor addresses	Check validity of vendor numbers, Check for P.O. boxes as addresses, Match vendor addresses to employee addresses, Flag large changes in vendor activity, Extract vendors having no tax ID no.
Ghost employees	Employees with same address	Check employee addresses for matches, Invalid Social Security numbers, Compare number of employees over years to insure changes match new minus

		terminated employees, Flag employees who have not used benefits
Unauthorized file access	Employees accessing unauthorized files or incompatible files	Compare log-ins to access rights and privileges
Inventory loss	Inventory adjustments	Flag all adjustments exceeding a set percentage, Check deliveries outside of regular hours, Check employee access to restricted areas during irregular hours
Vendor kickbacks to managers who order at high levels	Inventory levels exceed established peaks, Average inventories too high	Examine average inventory levels and high volume purchases, Establish an economic order quantity and require a signed override by inventory manager for larger amounts
Copying sensitive data files (intellectual property or personally identifiable information)	Employees accessing unauthorized files, Copy attempts on protected files	Compare copy attempts to rights and privileges
Financial statement fraud	Senior management making fraudulent entries	Flag all journal and ledger entries by executive management, Flag all entries that boost revenues over a certain percentage, Flag significant transactions with related party, Review sales recorded by Corporate Headquarters
Invalid earnings	Adjustments to estimates such as bad debt allowance, amortization of intangibles, insurance claims, etc.	Flag changes that exceed a set percent or ones made by executive management (should be made by lower level accountants)
Cash larceny	High differences between sales and cash receipts, High refunds, voids, A/R write-offs	Summarize information by employee and flag all large differences

Two examples of quantitative red flags would be irrational ratio analysis of Gross Margin Index and Sales Growth Index in order to determine if they fell outside of the industry norm. Horizontal analysis of the ratios could also point out trends and anomalies. Two examples of qualitative red flags would be significant insider sell-off of shares and opaque financial reporting and disclosures designed to confuse and mislead investors (Grove and Cook, 2004).

Figures 3 and 4 illustrate the possible application of forensic analysis. In Figure 3, Benford Analysis is used to analyze employee expenses. If the distribution of first-digits follows Benford's Law, then the resulting z-statistic would be low. The auditor might have a rule such as: do not investigate unless a digit has a z-statistic greater than 2. Such a rule can easily be altered over time.

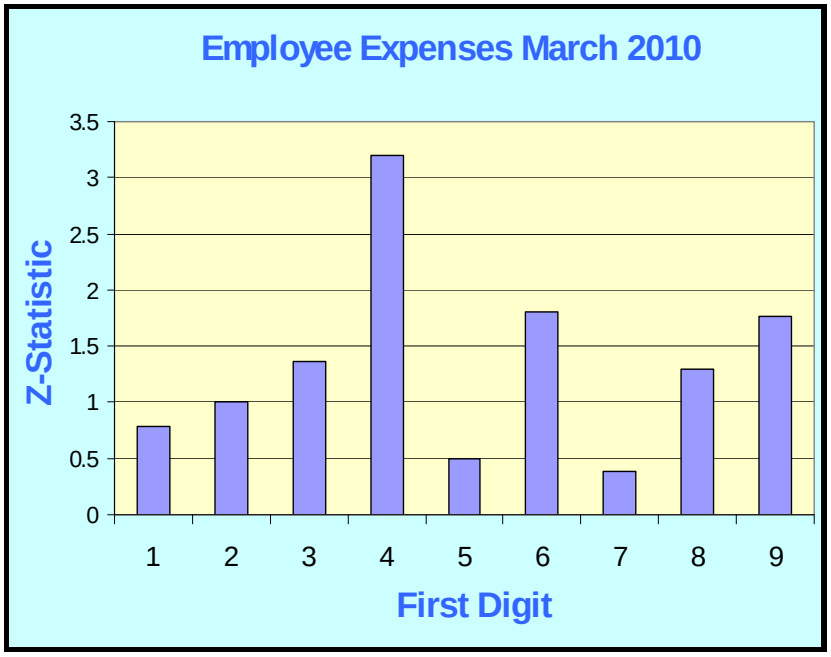


Figure 3: Applying Benford Analysis to Employee Expenses

In Figure 4, the number of transactions is compared to the percentage of known errors and outliers (for example, values that exceed the average by greater than 3 standard errors). Again, anomalies become quickly apparent allowing the auditor to focus the investigation on areas that are most likely to indicate a problem.

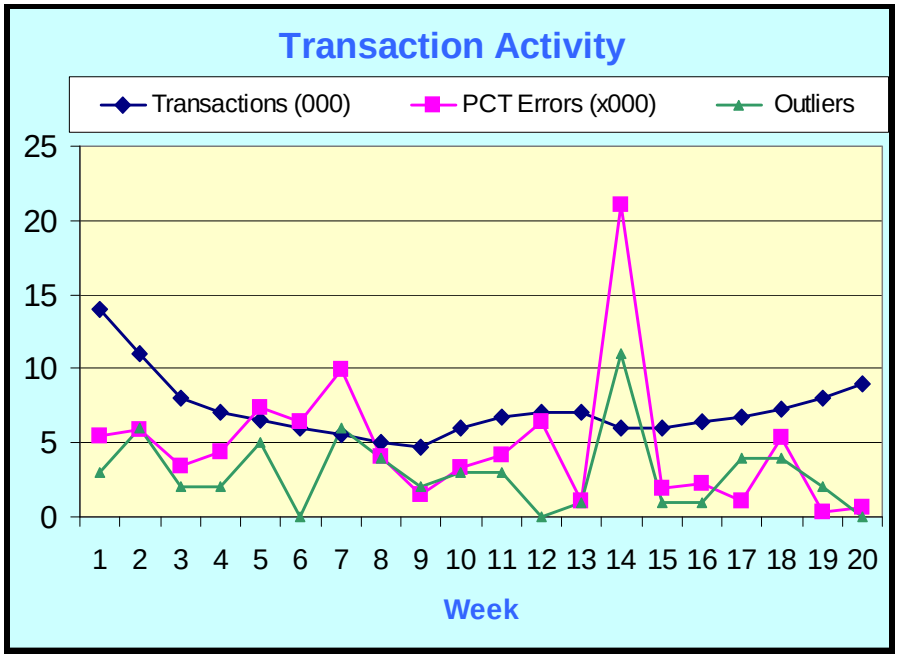


Figure 4: History of Transactions with Error Rate and Outliers

7. PROPOSITIONS

The following five propositions support the use of the FCA model as an effective method for deterring and detecting corporate fraud. They are rooted in practical realities that are likely to persist and place undue burdens on management, auditors and key stakeholders unless a technological solution is adopted.

With continuous auditing, auditors can design audit rules that test a large set of transactions (perhaps 100%) at determined time intervals. With FCA, the rules can test for errors, fraud, and the strength and presence of internal controls, while also performing some substantive tests. Results can be used to create compliance reports. Over time, experience-based adjustment of the audit rules can make them more efficient and effective. Anomalies and outliers can quickly indicate the presence of potential problems. Thus,

Proposition 1: Forensic continuous auditing will add efficiencies to the financial audit process.

Section 404 of SOX02 has elevated the need for extensive tests of IT internal controls that may require the expensive services of a third-party firm. Thus, the need for more comprehensive yet cost-effective approaches is recognized by external auditors. External auditors, however, must examine controls to insure

that insiders are not using their own knowledge to perpetrate frauds. According to the ACFE, accountants comprise the single group that commits occupational fraud. Owners and executives commit the most expensive frauds (ACFE, 2011).

By allowing the client's internal auditors to perform extensive testing of controls through continuous auditing procedures, the external auditor can avoid expanding the time-consuming and expensive substantive testing. Regulations require that certain substantive tests be performed. Auditing Standard AU 319.80, 81 states that "regardless of the assessed level of control risk, the auditor should perform substantive tests for significant account balances and transaction classes.'' By having access to increased data sets and allowing the client's internal auditors to perform more of the transaction testing through continuous auditing, the external auditor will be able to focus on more important activities that are more likely to lower risk. Thus,

Proposition 2: External auditors will perceive forensic continuous auditing positively.

PCAOB 5, *An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements*, has increased the reliance that external auditors can place on evidence generated by internal audit departments in an effort to reduce duplication of efforts and lower audit costs. FCA combined with CAATs are capable of monitoring internal controls for SOX02 compliance reporting and uncover areas of higher audit risk. As external auditors rely more on the internal audit and client's automated controls and governance testing mechanisms, less time will be required of external auditors or IT auditors. Additionally, fewer requests for ad hoc data sets will be made of the IT department. By having an established process in which audit rules can be increased and modified over time to improve the quality of the results, the internal auditors will play a higher role in the assurance process and be viewed more favorably by the audit committee and by management.

Proposition 3: Internal auditors will perceive forensic continuous auditing positively.

Management can be expected to view a system that continuously audits for fraud positively because it supports compliance in a cost effective manner. As mentioned above, it will allow more work to be subsumed by the internal auditors thus decreasing costs and the time external auditors are on the premises. Furthermore, the external auditors can access and inspect data sets and reports remotely, avoid travel expenses, and not have to import data because the documentation and proof of compliance will already exist.

Management might also take a human resources view towards forensic continuous auditing. SOX02 has made acquiring IT auditors even more difficult and the number of qualified individuals is relatively small. The number of

accountants with a Certified Information Systems Auditor license is less than 50,000 globally and all companies and accounting firms compete for these individuals (Kuhn and Sutton, 2010). Reducing the necessity for IT auditors will place less strain on human resources and commensurate salary levels.

Finally, management will value the ability to phase-in FCA on an application-by-application basis and expand the number of audit tests over time. Thus,

Proposition 4: Management will perceive forensic continuous auditing positively.

SOX02 requires management to evaluate and attest to the effectiveness of an internal control system (Arrens et al., 2006). Under increased regulatory scrutiny and facing increased audit costs management will seek cost-effective approaches to the detection of transaction errors and fraudulent activities. Increased penalties for fraud and the low percentage of fraud that is uncovered by auditors will make continuous auditing attractive as a forensic tool. Fraud deterrence is recognized as an important management objective. To prevent fraud, it is imperative that internal controls be tested continuously and that audit rules are established to uncover fraudulent events. This can be accomplished by examining a large percentage of the transactions and system events.

SAS 56, *Analytical Procedures*, requires that auditors perform analytical procedures during the planning and final reporting stages of the audit (AICPA, 1988). Analytical reviews, however, may not be effective at detecting frauds. Even large embezzlements may not have a material effect on the earnings of a large corporation and may escape discovery during a regularly scheduled audit (Wells, 2011). FCA, however, provides the ability for auditors to perform a multitude of analytical procedures over all transactions and significantly increases the possibility that errors and suspicious transactions are flagged (Rezaee et al., 2002). Properly constructed systems could perform hundreds of different analytical tests on a large number of transactions daily. Each test would be intended to seek out red flags. For example, delivery dates could be examined for times when deliveries are not normally made (holidays, weekends, after hours, etc.) and selected transactions would then be reviewed.

FCA also allows for special alarms called “audit hooks.” These are audit rules that snare transactions of a suspicious nature and allow for real-time intervention. A common example is when someone travels abroad and uses a credit card outside the normal venue. An audit hook captures the first use of the card in the foreign venue and immediately alerts a representative who then decides how to handle the transaction. One response is to attempt to contact the cardholder by phone or email. The response can take less than one minute. The hooks are highly effective at detecting and deterring possible fraudulent activities (Romney and Steinbart, 2008). Thus,

Proposition 5: Management will positively perceive the forensic continuous auditing model as an effective and efficient forensic tool.

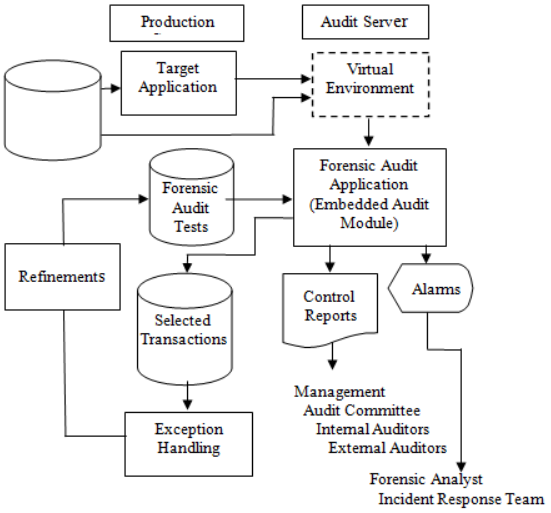
8. THE FORENSIC CONTINUOUS AUDIT SYSTEM

The FCA system is shown in Figure 5. Note that the Forensic Audit Application module functions as an embedded audit module but is outside the actual production version and can be applied to different applications eliminating the necessity of building separate embedded audit modules.

The Forensic Audit Application works with a cloned copy of the actual application using actual transactions but does not alter actual accounts or affect the performance of the system. The forensic tests are performed within a short period of time after the actual processing. This could be within minutes or within a week. Auditors must weigh the benefits and risk with the costs. Higher risk transactions would require more immediacy. In any event, there will be a more timely and thorough examination than under traditional audit approaches.

Sensitive audit tests can trigger alarms that request immediate response. Otherwise, selected transactions are saved and reports created for scheduled reviews. A phased approach would be based on creating a tested system that could be copied for other applications. Because invoking the tests within the production version of the application could reduce performance significantly, performing the tests in the background is preferred.

Some analysis of selected transactions may indicate the need for deeper inquiry. Extended analysis could be performed using a CAAT such as ACL or IDEA.



The target application is cloned to the audit server creating a virtual environment. The actual transactions are run on the audit server.

Forensic tests are applied to all transactions which may or may not be erroneous or fraudulent but are selected for review.

Selected transactions are stored for retrieval and archival. Control reports are created for review of selected transactions. Some transactions fail sensitive rules that trigger alarms and are made available for immediate review.

Qualified forensic analysts evaluate exceptions and suspicious transactions.

Examination of trends and anomalies allow auditors to refine fraud audit tests.

Figure 5: Forensic Continuous Auditing System

Future Research Considerations

Future research could examine various unknown aspects of forensic continuous auditing. First, and foremost, what is the true cost of implementing a full-scale model as presented in the paper. Surveys have shown that many companies have implemented CA to some extent but there is no mention in research of specific cost-savings. By understanding the cost-savings better, many companies would be more likely to adopt the model.

Second, researchers could examine the effectiveness of various audit tests, especially those that would indicate the override of controls that often lead to the more expensive financial statement fraud. By identifying and sharing effective audit rules, companies could more quickly realize the benefits of forensic CA. Future emphasis should be focused on preventive and detective rules as they assist internal auditors and the controller in ascertaining the likelihood of threats and identifying the source of threats.

9. CONCLUSIONS

The role of audits is clearly important and can have a strong preventive effect on fraudulent behavior, but audits alone cannot be relied upon exclusively for fraud detection and, with the increase of transactions processed, may not be an effective mechanism for uncovering errors or misuse. Experience has shown that the traditional audit is not an effective mechanism for uncovering fraud. Auditors and managers are faced with increased pressure to tighten internal controls and reduce corporate risks. At the same time, information systems are becoming increasingly

more complex and larger sets of transactions are being processed. Evidence exists that when faced with advanced technology auditors often resort to manual approaches that are less effective at detecting fraud or material misstatements. Using sophisticated audit tests and a graphical presentation of possible inconsistencies, auditors have a higher chance of preventing problems with internal controls or detecting them when they occur. Although continuous auditing is an attractive solution, many companies have failed to embrace it because of implementation issues and lack of trained auditors. This paper presents cogent reasons for adopting a system of forensic continuous auditing. Based on five propositions, an approach is presented that is manageable and scalable and can be introduced in phases. By using the continuous auditing approach, managers can be assured of transaction integrity and auditors can be relieved of some of the burdens of repetitive testing of controls and balances, allowing auditors to focus on matters that are more likely to reduce risk. Although embedded audit modules are used in some firms, this paper recommends the use of a cloned copy of the applications. The FCA still takes place at about the same time as the actual transaction processing and the difference from real-time is negligible. Examining relationships of revenues items with other associated financial and operating items increases the ability of auditors to uncover instances in which management may have used system overrides to introduce fictitious revenues. By investigating suspicious trends and outliers, auditors can decrease the opportunity for manipulation.

10. REFERENCES

Alali, F., G. H. Grant and K. C. Miller. 2008. IT Control Deficiencies that Impact Financial Reporting. *Internal Auditing*, Vol. 23 (4), pp. 28-37.

Albrecht, C. C., W. S. Albrecht, and J. G. Dunn. 2001. Can Auditors Detect Fraud. *Journal of Forensic Accounting*. Vol. II, pp. 1-12.

Aldhizer, G. R., and J. D. Cashell. 2006. Automating the Confirmation Process: How to Enhance Audit Effectiveness and Efficiency. *The CPA Journal.* Vol. 76 (4), pp. 28–32.

Alles, M. G., A. Kogan, and M. A. Vasarhelyi. 2008. Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations. *Journal of Information Systems*, Vol. 22 (2), pp. 195–214.

Alles, M. G., A. Kogan, and M. A. Vasarhelyi. 2002. Feasibility and Economics of Continuous Assurance. *Auditing: A Journal of Practice & Theory.* Vol. 21 (1), pp. 125–138.

Alles, M. G., F. Tostes, M. A. Vasarhelyi, and E. Riccio. 2006. Continuous Auditing: The USA Experience and Considerations for its

Implementation in Brazil. *Journal of Information Systems and Technology Management*. Vol. 3 (2), pp. 211-224

American Institute of Certified Public Accountants (AICPA). 2001. *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit. Statement of Auditing Standards No. 94*. New York NY: AICPA.

_____. 2002. *Consideration of Fraud in Financial Statement Audit. Statement of Auditing Standards No. 99*. New York NY: AICPA.

_____. 1995. *Consideration of Internal Control in a Financial Statement Audit. Statement of Auditing Standards No. 78*. New York NY: AICPA

_____. 1988. *Analytical Procedures. Statement of Auditing Standards No. 56*. New York NY: AICPA

Arens, A.; Elder, R.; Beasley, M. 2006. Auditing and Assurance Services: An Integrated Approach. *Pearson Prentice Hall.*

Association of Certified Fraud Examiners (ACFE) *2010 Report to the Nation on Occupational Fraud and Abuse*.

Audit Command Language (ACL) Downloaded January 4, 2011 from: http://www.acl.com/solutions/fraud_detection.aspx

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants (CICA/AICPA). 1999. *Continuous Auditing*. Research report. Toronto, Canada: CICA.

Caster, P. and R. Sriram. 1996. An Investigation of Accounts Receivable Confirmation Process Timing. *Auditing: A Journal of Practice & Theory*. Vol. 15 (1), pp. 135–141.

Charles Rivers & Associates. 2005. *Sarbanes-Oxley Section 404 Costs and Remediation of Deficiencies: Estimates from a Sample of Fortune 1000 Companies*. Downloaded January 5, 2011 from: http://www.sec.gov/spotlight/SOX02comp/SOX02comp-all-attach.pdf.

Chen, C. and J. T. Sennetti. 2005. Fraudulent Financial Reporting Characteristics of the Computer Industry Under a Strategic-Systems Lens. *Journal of Forensic Accounting*. Vol. VI, pp. 23-54.

Debreceny, R. S., G. L.Gray, J. J. Ng, K. S. Lee, and W. Yau. Fall 2005. Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Functionality. *Journal of Information Systems*. Vol 19 (2), pp. 7–27.

Grant, G. H., K. C. Miller and F. Alali 2008. The Effect of IT Controls on Financial Reporting. *Managerial Auditing Journal*. Vol. 23, (8), pp. 803-823.

Groomer, S. M., and U. S. Murthy. 1989. Continuous Auditing of Database Applications: An Embedded Audit Module Approach. *Journal of Information Systems*. Vol. 3 (1), pp. 53-69.

Grove, H. and T. Cook. 2004. Lessons for Auditors: Quantitative and Qualitative Red Flags. *Journal of Forensic Accounting*. Vol. V, pp. 131-146.

Hermanson, D. R. , B. Moran, C. S. Rossie and D. T. Wolfe. 2006. Continuous Monitoring of Transactions to Reduce Fraud, Misuse, and Errors. *Journal of Forensic Accounting*. Vol. VII, pp. 17-30.

Hoffman, T. 2004. IT Auditors Coveted, Hard to Find. *Computerworld*, Vol. 38 (18), pp. 1-16.

Kuhn, J. R. Jr. and S. G. Sutton. Spring 2010. Continuous Auditing in ERP System Environments: The Current State and Future Directions. *Journal of Information Systems*. Vol. 24 (1), pp. 91-112.

Janvrin, D., D. Bierstaker and D. J. Lowe. Spring 2009. An Investigation of Factors Influencing the Use of Computer-Related Audit Procedures. *Journal of Information Systems*. Vol. 23, (1), pp. 97–118.

Johnson, C. B. and T. C. Ireland. 2007. An Empirical Examination of Manipulation in Components of the Income Statement. *Journal of Forensic Accounting*. Vol. VIII, pp. 1-28.

Lanza R. B., and S. Gilbert. 2007. A Risk-Based Approach to Journal Entry Testing. *Journal of Accountancy*. Vol. 204, pp. 32–35.

Nigrini, M. J. 2006. Monitoring Techniques Available to the Forensic Accountant. *Journal of Forensic Accounting*. Vol. VII, pp. 321-344.

Nondorf, M. E., Singer, Z. and You, H., (February 2011) A Study of Firms Surrounding the Threshold of Sarbanes-Oxley Section 404 Compliance.

AAA 2008 Financial Accounting and Reporting Section (FARS) Paper. Available at SSRN: http://ssrn.com/abstract=1004965

Rezaee, Z., A. Sharbatoghlie, R. Elam, and P. L. McMickle. 2002. Continuous auditing: Building
automated audit capability. *Auditing: A Journal of Practice & Theory*. Vol. 21 (1), pp. 147–163.

Roth, J. and D. Espersen. 2003. *Internal Audit's Role in Corporate Governance: Sarbanes-Oxley Compliance*. Altamonte Springs: The Institute of Internal Auditors Research Foundation.

Li., S., S. Huang and Y. G. Lin. Fall 2007. Developing a Continuous Auditing Assistance System based on Information Process Models. *Journal of Computer Information Systems*. Vol. 48 (1), pp. 2-13.

Oringel, J. and G. R. Aldhizer. Fall 2009. Continuous Auditing and Monitoring: Enhancing the Efficiency and Effectiveness of Auditing and ERM. *Internal Auditing*. Vol. 24 (5), pp. 17-26.

Public Company Accounting Oversight Board (PCAOB). 2007. Auditing Standard No. 5: *An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statement*.

Romney, M. B. and P. J. Steinbart. 2008. *Accounting Information Systems, 11th ed.* Prentice-Hall.

G. S. Smith. 2005. Computer Forensics: Helping to Achieve the Auditor's Fraud Mission?. *Journal of Forensic Accounting*. Vol. VI, pp. 119-134.

Vasarhelyi, M. A, M. Alles, and A. Kogan. 2004. Principles of Analytic Monitoring For Continuous Assurance. *Journal of Emerging Technologies in Accounting*. Vol. 1, pp. 1–21.

Wells, J. T. 2011. *Principles of Fraud Examination*. Hoboken, NJ: John Wiley & Sons.