THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 4 | Number 1 Article 3

2009

Defining a Forensic Audit

G. S. Smith
Southeastern Oklahoma State University

D. L. Crumbley
Louisiana State University

Recommended Citation

Smith, G. S. and Crumbley, D. L. (2009) "Defining a Forensic Audit," *Journal of Digital Forensics, Security and Law*: Vol. 4 : No. 1 , Article 3.
DOI: https://doi.org/10.15394/jdfsl.2009.1054
Available at: https://commons.erau.edu/jdfsl/vol4/iss1/3

Defining a Forensic Audit

G. Stevenson Smith, Ph.D., CPA, CMA
John Massey Endowed Chair and Professor of Accounting
Southeastern Oklahoma State University
Durant, OK 74701
Phone: 580.745.2490
Fax: 580.745.7485
E-mail: sgsmith@se.edu

D. Larry Crumbley, Ph.D., CPA, Cr. FA, CFD, FCPA
KPMG Endowed Professor
Louisiana State University

ABSTRACT

Disclosures about new financial frauds and scandals are continually appearing in the press. As a consequence, the accounting profession's traditional methods of monitoring corporate financial activities are under intense scrutiny. At the same time, there is recognition that principles-based GAAP from the International Accounting Standards Board will become the recognized standard in the U.S. The authors argue that these two factors will change the practices used to fight corporate malfeasance as investigators adapt the techniques of accounting into a forensic audit engagement model.

Keywords: auditing, fraud examination, forensic audits, forensic accounting, financial reporting.

1. DEFINING A FORENSIC AUDIT

To successfully exercise good corporate governance, there is a need for internal controls and one aspect of these controls relates to financial oversight. Unfortunately the number of financial frauds that have been continually perpetrated within U.S. companies raises serious questions as to whether traditional financial controls are working.[1] "Is the traditional audit model still

[1] The 2002 accounting scandals include: AOL, Adelphia, Bristol-Myers Squibb, Charter Communications, Computer Associates, Duke Energy, Dynegy, El Paso Corporation, Enron, Freddie Mac, Global Crossing, Halliburton, Harken Energy, HealthSouth, Lucent Technologies, Merrill Lynch, Quest Communications, Reliant Energy, Sunbeam, Tyco International, Waste Management, Inc. and World Com. The 2003 accounting scandals include: Royal Ahold Parmalat, and Calisto Tanzi. The 2005 accounting scandals include AIG. During 2006 and 2007, accounting scandals are related to the backdating of corporate stock options from companies such as Monster Worldwide, Inc. Dell has been added to the list in 2007 as a result of a kickback

doing its share in providing oversight over financial activities?" Today the answer might be, "not very well, but what other choice is there?" Questions about the ability of the audit-reporting model to provide reasonable financial oversight and the broader acceptance of principles-based accounting methods have the potential to create a new approach to risk assurance. This paper argues that forensic auditing, which is based on the practices of forensic accounting, is the best choice for reducing financial malfeasance in a principles-based accounting world.

2. A PRINCIPLES-BASED WORLD IS COMING

Forensic auditing is focused on the identification, interpretation, and communication of the evidence of underlying strategic economic and reporting events.[2] It not single-event based, like a fraud examination, and a forensic audit is not used to render an audit opinion. As such, forensic audits are easily adapted to a principles-based accounting environment with broad guidelines applied to a variety of accounting investigations without using rule-based audit approaches or more narrowly-focused fraud practices.

Principles-based methods have been receiving more recognition as an alternative in U.S. accounting practices (Global Public Policy Symposium 2008; Shortridge and Myring 2004) as there has been an increased emphasis for more unified worldwide accounting practices.[3] In the white paper, *Principles-Based Accounting Standards* (Global Public Policy Symposium 2008) a call is made by the Big Four along with Grant Thornton and BDO International for the adoption of "reasonable judgment" in the application of accounting principles.

Principles-based generally accepted accounting principles (GAAP) are being developed by the International Accounting Standards Board (IASB). Continued globalization of the business economy has resulted in the adoption of these accounting standards by 100 countries including five G8 countries along with plans for adoption by a number of other countries within the next five years. The IASB's accounting standards, known as the International Financial Reporting

---

scheme. Frauds growing out of the sub-prime mortgage meltdown in 2008 and 2009 are too numerous to list.

[2] The Public Company Oversight Board (PCAOB) issued Release No. 2007-001 in January 2007. The Release defines forensic accounting as operating outside the courtroom and applying "special skills in accounting, auditing, finance, quantitative methods, certain areas of the law, and research, and investigative skills to collect, analyze, and evaluate evidential matter and to interpret and communicate findings (Public Company Oversight Board 2007).

[3] Principles-based practices use the following criteria along with less detailed rule making: (Global Public Policy Symposium 2008): (1) Faithful presentation of economic reality; (2) Responsive to users' needs for clarity and transparency; (3) Consistency with a clear conceptual framework; (4) Based on an appropriately-defined scope that addresses a broad area of accounting; (5) Written in clear, concise and plain language; (6) Allows for the use of reasonable judgment.

Standards (IFRS), are being considered for adoption as GAAP in the United States by 2014.[4] The SEC has been holding hearings to assess opinions about the timing and form of adoption in the United States.[5] The IASB's standards do not use the detailed rule-based approach found in U.S. GAAP. For example, U.S GAAP requires that a capital lease be recognized when the lease term is equal to or greater than 75% of the asset's economic life; while IFRS guidelines only require such treatment when the lease term is a "major part" of the asset's economic life.[6] The term "major part" needs to be decided by the accountant. Additionally, deferred taxes under U.S. GAAP are recognized in full; whereas under IFRS, they are recognized when it is "more likely than not" that they will be realized.[7] Thus, the accountant's judgment is more dominant in evaluating the underlying nature of a financial transaction under international standards.

These changes are expected to affect the rule-based formats used in U.S auditing and GAAP procedures as well as provide an opportunity for the implementation of forensic audits. Forensic audits fit within a principles-based approach as they require the application of professional judgment to identify the underlying nature of unstructured and unreported financial transactions. A forensic auditor must assess the underlying nature of transactions and apply a deductive mindset using professional judgment as the primary source for interpreting accounting events. As the evaluation of accounting events becomes more strongly based on judgment, forensics has the potential of supporting such an approach by monitoring corporate activities for "economic reality" and "economic consequences." [8] Further, the implementation of principles-based methods under forensic auditing is likely to be more politically acceptable than trying to change decades of rules-based practices under U.S. auditing standards.

3. LEGAL LIABILITY AND RULE-BASED PRACTICE

The accountant's legal liabilities arising from the performance of audits had a

[4] The SEC will allow certain domestic companies to use IFRS as early as December 31, 2009. The 2014 date for other companies may vary with specific SEC phrased-in timetable objectives.

[5] The most recent Securities and Exchange Commission Roundtable on the topic "Practical Issues Surrounding the Use of IFRS in the U.S. in Recent Years and its Potential Expanded Use in Future Years" was conducted in Washington, D.C. on December 17, 2007. See: http://www.sec.gov/spotlight/ifrsroadmap.htm

[6] The IASB and the FASB are reviewing the differences in their approaches to lease accounting as found in Statement of Financial Accounting Standards No. 13, *Accounting for Leases*, and International Accounting Standard 17, *Leases*, respectively. To help overcome some of these differences, the FASB issued a Discussion Paper on March 19, 2009 (No. 1680-100) titled *Leases: Preliminary Views*.

[7] See Statement of Financial Accounting Standards No. 109, *Accounting for Income Taxes*, and International Accounting Standard 12 *Income Taxes*.

[8] The Global Report (2008) views forensics as a means of measuring economic reality and projecting economic consequences of corporate events.

significant influence on the development of rule-based practices followed in the United States. The purpose of rules-based accounting has been "to address as many potential contingencies as possible" (May 1937). Still, company officials bent on defrauding stockholders have evaded these rules, and the accountant's legal liabilities have not been diminished.

Rule-based approaches have been slowly developed over the decades by accounting and auditing standard-setting bodies. The result is a detailed set of rules that are used to cover almost every after-the-fact recognized or developing accounting problem and transaction. This approach was not always practiced. At one time, it was believed the subjective nature of accounting made the judgment of the accountant superior to a set of detailed rules for recording complex transactions. George May, whose roots as an accountant were in the United Kingdom, believed the "substance of the accounts may and often should vary according to the purpose for which the accounts are required" (May 1950).[9] May stated that "...no amount of standardization will either (a) make an understanding of the nature of accounting process less necessary to a proper interpretation of such determinations, or (b) convert those determinations into findings of fact" (May 1950). May's arguments were not successful in influencing the direction taken by the accounting profession, and the application of GAAP and SASs changed a principles-based approach relying on the judgment of the accountant into a practice of closely following a set of detailed prescriptions.[10] Interpretation of management's financial actions into financial statements was largely replaced with applying a comprehensive and extensive set of accounting and auditing rules to prepare those financial statements. Unfortunately, this approach has allowed corrupt financial executives to also read the rules and find the loopholes or understand the weaknesses in the GAAP model and circumvent them.

There are two major reasons that rule-making came to predominate in the U.S. accounting profession. One was to show government agencies, such as the Securities and Exchange Commission (SEC), that the rules of accounting practice were being addressed by the profession. Still the enactment of the Securities Acts

[9] George O. May was a senior partner of Price Waterhouse & Company for almost thirty years and a well-respected accounting practitioner. He was the first chairman of the Committee on Accounting Procedure (CAP) of the American Institute of Accountants. CAP influenced the formulation of early U.S. accounting principles. He authored over a hundred articles that can be traced back to 1906 in the *Journal of Accountancy,* and thus he exercised a strong voice in influencing accounting practices.

[10] In 1964, the AICPA formed a committee known as the Special Committee. The role of the Special Committee was to determine how departures from AICPA accounting standards in effect at the time should be handled. The recommendations of the Special Committee and a vote of the AICPA resulted in changing the manner in which accounting pronouncements were applied in practice. Prior to the vote pronouncements were considered important, but not important enough to override the auditor's best judgment. After the vote, accounting rules were considered authoritative.

have always created the fear the SEC would hand down accounting principles through "bureaucratic edict" (Brewster 2003). Another reason was the generally perceived notion that closely following accounting rules would reduce an accounting firm's legal liability arising from undiscovered financial malfeasance of a corporate client. It was argued that if the rules were closely followed such a practice would provide for the legal protection of the accounting profession.[11] The SEC has largely allowed the profession to set accounting and auditing standards until recently, but the profession has not been successful in avoiding the damaging liability lawsuits arising from their corporate client's fraudulent activities.

4. A POSSIBLE SOLUTION: FORENSIC AUDITS

Auditor's legal liabilities for not discovering their client's fraudulent financial actions are simply not going to disappear. It is hard to understand how the liability for undiscovered frauds or other malfeasance can be reduced by continuing to strongly rely on the present rule-based, audit-reporting model. When forensic accounting practices are incorporated into a separate forensic audit, they have the potential to overcome problems associated with identifying financial malfeasance within the traditional audit-reporting model.

Recently, the Big Four along with Grant Thornton and BDO International released a white paper entitled "Serving Global Capital Markets and the Global Economy" herein the "Global Report" (Global Public Policy Symposium 2006). The Global Report is concerned with the legal liabilities accounting firms are facing from a host of expanding lawsuits based on stockholders' and others' losses from after-audit negative financial events such as fraud. To counter this hostile legal climate and protect the firms from liabilities judgments, the Global Report's authors suggest that all public companies have *forensic audits*. The writers of the Global Report place forensic audits under the practices of the traditional audit-reporting model and view a forensic audit as a fraud examination. Under those conditions, such a periodic "forensic audit" would be time consuming and expensive as noted in the Global Report.

Yet, forensic audits do not have to be part of the traditional audit-reporting model. Although the objectives and definition of a forensic audit have not been clearly defined in the Global Report, here a forensic audit is considered to be an application of methodologies and technologies by an independent entity used to obtain a detailed understanding of the underlying economic risks facing an organization.[12] Today's technologies allow for cost effective means to

[11] This perspective does not allow for blindly following standards and principles and consequently being absolved from all legal liability (See Tinker 1986, p. 105).

[12] The PCAOB has stated that "forensic audits can be performed to achieve various objectives and can include a variety of different procedures" (Public Company Accounting Oversight Board 2007b). Thus, forensic audits have been discussed but not defined in any set of established auditing standards. See: (www.pcaobus.org/Standards/Standing_Advisory_Group/Meetings/2007/02-

continuously monitor (not spot check) corporate activities under forensic audit practices.[13] The Global Report is written as a defense of the accounting profession and opposes large legal settlements against accounting firms, but the Global Report's call for forensic audits should be viewed as a first strategic step to integrate principles-based GAAP and risk assurance.

5. CONCEPTUAL BASIS: FORENSICS ACCOUNTING, FRAUD EXAMINATION, AND AUDITS

Before describing the professional practices followed in forensic auditing, the contrasting concepts underlying forensic accounting, fraud examinations, and traditional auditing need to be briefly compared. Forensic accounting proactively integrates accounting, criminology, computer forensics (investigations), litigation services, and auditing investigative services into the investigation of a broad range of future-oriented business problems as shown in Figure 1 (Smith and Crumbley 2009) . Areas of investigation in forensic accounting are broad and include fraud examination, due diligence reviews, risk assessment, detection of financial statement misrepresentation, cybercrimes, illegal money transfers, modeling risk

---

22/Forensic_Audit_Procedures.pdf.). Also (http://www.cfonet.com/article.cfm/8759510?f=search)

[13] Beyond data mining software, such as ACL (http://www.acl.com) and IDEA (http://www.audimation.com), there are a number of software programs that can used to analyze the risks facing an organization. For examples of cost effective continuous monitoring see: (1) Confident Compliance (https://www.itcinstitute.org/display.aspx?id=347) a software package that continuously monitors process controls such as transaction rules in an organization. Such a technology approach reduces the cost of complying with Sarbanes-Oxley statutes. (2) Visual Analytics' software package called Visual Links (http://www.visualanalytics.com) uses a graphical screen to uncover patterns, associations, and relationships among masses of unrelated data. (3) Maltego (http://www.paterva.com/web2/maltego/maltego-2.html)is a software monitoring program used to establish links between corporate employees and others with whom they communicate to determine if they are violating corporate guidelines. (4) ISYS Search Software (http://www.isys-search.com) used to make forensic searches of e-mails and information on hard drives over the entire intranet. (5) RFID technologies that raise alerts when company notebooks are removed from company premises. (6) NetMap Analytics (http://www.netmapanalytics.com)used for mapping unrecognized relationships by mapping common links. (7) SpectorSoft CNE Investigator (http://www.spectorcne.com) surveillance software that records everything that employees do on the Internet. (8) PyFlag (http://www.pyflag.net) is a tool that is used to analyze large volumes of log files. Background arguments for using these approaches can be found in the paper: *Empowering Board Audit Committees: Electronic Discovery to Facilitate Corporate Fraud Detection* (Michaud, Dutton, and Magaram 2006). The authors recommend the continuous monitoring of e-mail messages within a corporation. Once an activity was identified as possibly fraudulent, additional authorization would be needed to forensically examine any electronic evidence. For examples of computer forensic software see the *Buyer's Guide to Audit, Anti-Fraud, and Assurance Software* (Brooks, Goldman and Lanza 2007).

assessment, and the identification of earnings management.[14]

The study of criminology represented in Figure 1 deals with theories that cause crime to develop, such as conflict theory, natural choice theory, and social control theories. Topics include corporate crime, corporate culture reviews, and interview techniques.[15] The circle represented by accounting is the basic accounting and financial understandings and the foundational skills students develop as they advance through their undergraduate university accounting courses. This basic skill set allows students to enter a fraud/forensic curriculum. The next skill set in Figure 1 is investigative auditing. In this representation, fraud examination is considered to be part of investigative auditing along with the traditional investigative auditing areas centered on transaction analysis applied within inventory fraud or cash theft, for example. Also included in Figure 1 is a litigation skill set. Litigation includes the ability to understand the discovery process, rules of evidence at the Federal and state levels, the difference between civil and criminal proceedings, differences between being an attorney in the courtroom compared to being an accountant, acting as expert witness, valuation services, and preparing electronic data for trial. Finally accounting/computer forensic skills surround the other skill sets. This skill set includes collecting and working with electronic data without compromising or destroying the data needed for an investigation. In addition, it deals with an understanding electronic information risk and locating an electronic footprint used to create either bogus electronic or paper records, for example (Smith 2005). Today developing such a skill set is important because "92 percent of new data is created electronically and 70 percent of that data never migrates to paper" (Kahan 2006). It is important to note that all the skills of the forensic accountant are applied when a forensic audit is performed.

Unlike forensic accounting, fraud examination is a reactive investigation launched to identify specific violations of fiduciary relationships based on an individual's suspicions that a fraud has occurred or could occur. Fraud investigations are singularly concerned with identifying a perpetrator and co-conspirators who benefited from fraudulent activities. Such investigations include specific reviews of misrepresentations and concealment of material financial facts, cash larceny, payroll schemes, expense reimbursement schemes, inventory theft, bribery, and

[14] For an example of the range of service that can be included under a definition of litigation service see: M. Wagner and P. Frank, *Management Advisory Services Technical Consulting Practice Aid 7: Litigation Services*, New York: AICPA, 1986.

[15] The guide, *Managing the Risk of Fraud: A Practical Guide*, herein the Guide, (Institute of Internal Auditors 2008) has outlined practices in fraud risk management programs. Although not calling for corporate culture reviews, the Guide stresses the importance of corporate culture in setting the ethical tone within an organization.

fraudulent financial statement schemes.[16] Once the nature of the fraud is identified, these investigations become very transaction oriented.

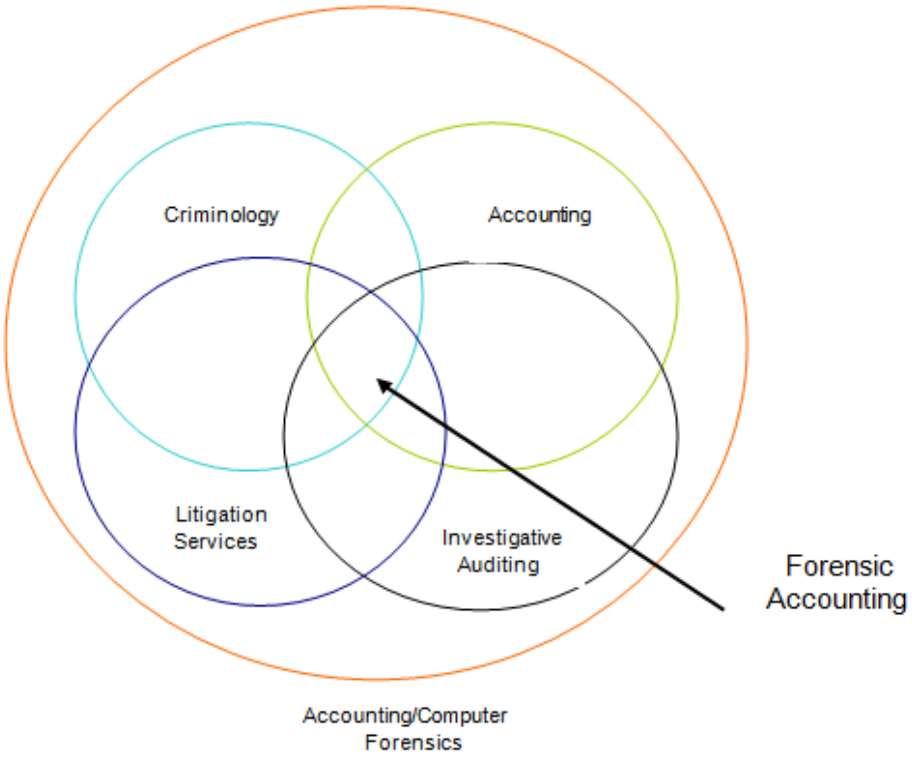

Figure 1. Skill Sets in Forensic Accounting

Financial auditing is based on providing periodic assurances that account balances are statistically and materially accurate, internal controls are adequate, and accounting rules are followed. The perspective in an audit engagement is less adversarial than in a fraud or forensic investigation, and it is based on a series of rules and guidelines until recently issued by the American Institute of Certified Public Accountants (AICPA) and currently by the Public Company Accounting Oversight Board (PCAOB) for public companies. Financial audits strongly rely on tests of internal financial controls to determine the extent of required transaction testing, and the financial audit is performed in a documented step-by-step fashion. Such an approach is necessary to issue an audit opinion and to show that properly documented procedures were followed in order to answer any after-audit legal

[16] The Association of Certified Fraud Examiners (http://www.acfe.com) supports fraud examination through its programs and provides training on topics such as those listed here. The ACFE's website contains a full listing of fraud examination topics.

inquiries about the audit. The audit becomes a rule-based process as somewhat legalistic practices are followed. Table 1 highlights several differences between auditing, fraud examinations, and forensic accounting.

Characteristic:	Audit	Fraud Examination	Forensic Accounting
Time Perspective:	Historical	Historical	Future and Historical
Primary Focus:	Periodic	Reactive	Proactive and Ongoing
Investigation Scope:	Narrow	Narrow	Broad Ranging
Main Work Product is:	Audit Opinion	Fraud Case Report	Forensic Audit Report
Main Responsibility to:	Company and Public	Defrauded party	Concerned principal or third party
Guidelines are:	Rules-based	Principles-based; under audit rules, it is rule-based	Principles-based
Purpose of Report:	Ensure GAAP is followed	Identify perpetrator of fraud	Fraud Risk Assessment and Strategic Services
Professional Stance:	Non-adversarial	Adversarial	Adversarial and non-adversarial

Table 1. Contrasting Auditing, Fraud Examination, and Forensic Accounting

In comparing audits, fraud examinations, and forensic accounting, it should be recognized that forensic accounting is forward-looking. For example, a forensic analysis is used to determine anomalies by establishing a financial baseline and modeling deviations of projected results from the established baseline. The forensic analysis is a continuous process that uses technology to identify suspicious activities occurring in company or other targeted environment. In contrast, fraud examinations focus on the present and the past to determine how crimes were committed. Similarly, audits review financial reporting in the past fiscal period, and in that sense, an audit is similar to fraud examination. As, a singularly-focused subset, fraud examinations can easily fit within the scope of a traditional audit or a forensic audit.

In summary, forensic accountants may be engaged in preventing or identifying fraud, but generally forensic accountants are employed in a much wider variety of risk management engagements.

6. FRAUD AND FORENSICS IN PRACTICE

It is difficult for fraud examination and forensic accounting to effectively operate within the traditional auditor-client relationship. Fraud and forensic approaches do not assume the client will honestly follow any of the detailed rules of GAAP or that an audit check-off list for revenue recognition, for example, will lead to the discovery of financial misconduct.

When an independent fraud examination or forensic audit is performed, there is a high probability that an adversarial stance will be taken toward the subject of the investigation. If either of these investigations fall under the annual periodic procedures of the financial audit, the mindset of forensic or fraud practitioner must change to correspond with financial auditor-client relationship. As a result, forensic and fraud investigations must closely fit within the non-adversarial, step-by-step procedural practice of a financial audit. Such a change makes it difficult to apply the principle-based and flexible forensic and fraud techniques needed to identify the unpredictable criminal patterns used in committing and concealing financial crimes.

Shortly after the Enron, World Com, and Xerox debacles, fraud examination was given recognition under audit practices. Statement of Auditing Standards (SAS) No. 99, Consideration of Fraud in a Financial Statement Audit altered the general approach of the accounting profession toward fraud recognition. SAS No. 99 was issued by the AICPA and went into effect on December 15, 2002.17 Under the SAS, the rules for fraud investigation were expanded, and the auditor is expected to display a heightened attitude of professional skepticism throughout the audit. The auditor must identify the risks of material misstatement in the financial reports and write up the results of the analysis. Auditors must "brainstorm" to identify ways that fraud could be committed in the audited organization. The number of managers and employees questioned under the new rules has been increased. Yet all these fraud identification procedures are performed under the umbrella of a financial audit and its rule-based methodology. Notably, SAS No. 99 does not refer to forensic accounting.18 Thus, the AICPA viewed fraud as closely related to financial audits; more so than forensics. Fraud inquiries, in SAS No. 99, have a secondary role to the main audit engagement, and as a result, adversarial stances are muted under the auditor-client relationship.19

---

[17] *Consideration of Fraud in a Financial Statement Audit*. Statement on Auditing Standards Number 99, *Consideration of Fraud in a Financial Statement Audit* (Effective date on or after: December 15, 2002). AICPA, New York. SAS No. 99 supersedes SAS No. 82 which had superseded SAS No. 53 (issued in 1988).

[18] Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* AICPA, *Professional Standards*, vol. 1, AU sec. 316.50, par .50 refers to "forensics" once when it mentions the use of "forensic and information technology specialists." The SAS mentions the term "fraud" three hundred and eighty-five times.

[19] Release No. 2007-001 from the PCAOB was issued in January 2007 five years after the issuance of SAS No. 99. The Release adopted a critical tone regarding the

In 2002, Sarbanes-Oxley (SOX) legislation was enacted by the U.S. Congress in response to corporate fraud.[20] In light of the seemingly dismal record the AICPA had in establishing auditing standards to mitigate fraud scandals, SOX statutes took the role of setting auditing standards for public companies away from the AICPA and put it in the hands of the Public Corporation Accounting Oversight Board (PCAOB). The PCAOB is a semi-governmental board that operates under the purview of Securities and Exchange Commission (SEC).

The PCAOB's most recent audit guidance is found in Auditing Standard No. 5, (AS5) *An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements.*[21] AS5 emphasizes the need to examine internal controls in making fraud risk assessments. Thus, the PCAOB's pronouncements heavily rely on an examination of internal controls that basically mirror the methods followed in the SAS's previously issued by the AICPA. It is not being argued here that internal controls should be ignored. It is being argued that a strong and largely singular reliance on internal controls has not served as the means to significantly reducing corporate fraud and ensure that management's financial responsibilities toward corporate stakeholders are exercised.

The main focus of professional standard setters has been to incorporate a measure of fraud examination into the audit environment. At the present time, an audit engagement does not require the performance of any true forensic procedures.

7. IMPLEMENTING THESE PRACTICES IN A FRAUD CASE

The differences between the practices followed under audit, fraud examination, and a forensic audit can be examined through the review of a financial fraud.[22] The example chosen here is the Brightpoint fraud. Brightpoint executives committed a financial fraud to hide a substantial decrease in annual profits. The fraud involved a complex financial accounting conspiracy among high-level executives at two separate companies. The executives were familiar with auditing rules and GAAP, and they developed a falsified transaction that would meet all the requirements of those guidelines.

---

manner in which auditing firms were implementing their fraud responsibilities under SAS No. 99. For example, the PCAOB leveled criticism against the practice of using standard audit checklists as a means of checking for fraudulent corporate activities (Public Company Accounting Oversight Board 2007a).

[20] Sarbanes-Oxley Act of 2002, PL 107-204, 116 Stat 745. The act makes corporate officers responsible for earnings reports, forbids accounting firms from acting as consultants to accounting clients, and stiffens penalties for fraud.

[21] Public Company Accounting Oversight Board. Auditing Standard No. 5, *An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements* (Effective June 12, 2007).Washington, D.C.

[22] The forensic methods described here are specifically related to the Brightpoint fraud, and although they provide an indication of the nature of a forensic audit, they should not be considered as composing the entire set of practices followed in a forensic audit.

Brightpoint, Inc.

Brightpoint, Inc. is a firm with a global sales and distribution network of products such as handsets, PDAs, and software with total revenues of over $1 billion. Phillip Bounsall, (Executive Vice President, Chief Financial Officer and Treasurer) John Delaney (Chief Accounting Officer and Controller), and Timothy Harcharik (Director of Risk Management) were Brightpoint's top executives involved in a "round trip" financial fraud in 1999. In 1998, Brightpoint forecasted a $13 to $18 million one-time charge against its 1998 revenues. The charge was related to losses from the closure of Brightpoint's United Kingdom middle-man trading operations for their wireless products. The loss was reported as follows in its 1998 annual report:

Trading Charges

Through the end of the third quarter of 1998, the Company had been engaged in the business of trading wireless handsets. Trading involves the purchase of wireless handsets from sources other than manufacturers or network operators (i.e., trading companies) and the sale of those handsets to purchasers other than network operators or their representatives (also trading companies). At the beginning of the fourth quarter of 1998 the Company decided to cease its trading activities primarily because: (i) those activities were not consistent with its strategy of emphasizing relationships with wireless equipment manufacturers and network operators, (ii) because the margins earned on the trading activities were rapidly decreasing and (iii) the Company had increasing concerns about the business practices of many trading companies.

In connection with the discontinuance, the Company recorded a charge of approximately $17.7 million ($13.8 million net of related tax benefits) in the fourth quarter of 1998. This charge included approximately $3.0 million for employee termination costs and other costs related to the discontinuation of the trading division. Additionally, certain assets that related to the trading division were determined by the Company to be impaired and, accordingly, were written down to their estimated fair value resulting in a charge of approximately $14.7 million. These assets included accounts receivable generated from sales to trading companies, inventory prepayments to trading companies and inventories purchased from trading companies. The impairment of these assets is a result of actions necessary to discontinue the trading division and certain activities carried out by individuals and third party trading companies in 1998 that were inconsistent with the best interests of the Company.

Prior to the issuance of the annual report, it became obvious the trading loss was close to $29 million. In order to report the loss within the forecasted range in Brightpoint's 1999 annual report, Delaney and Harcharik purchased a "retroactive insurance" policy from American International Group, Inc. (AIG). In 1999, the receivable on the policy was used in covering $12 million in 1998 losses and show the reported loss within the forecasted range as well as hiding the round trip payment to AIG. The result of the deception was an overstatement of Brightpoint's income before taxes by 61 percent.

AIG is a large holding company whose subsidiaries sell a wide range of insurance products. Brightpoint negotiated an indemnity insurance policy in January 1999 with an AIG subsidiary. All the policy documents were pre-dated to August 1, 1998. The insurance policy was specifically structured to smooth annual income.

Phillip Bounsall, Brightpoint's Executive Vice President, Chief Financial Officer, and Treasurer, was aware and concurred with these financial misstatements. In 1996, Bounsall had stock options exercisable that could have been worth $713,152 if the stock values appreciated 10%. If the 1998 trading loss was recognized, his stock options would have lost significant value. The bonuses were based on profitability targets, revenue growth, and increases in stockholder value, all of which would be seriously affected if there were a 61% decrease in operating profit from the UK closure. The entire purpose of this financial fraud was to enter into an insurance agreement whereby losses of approximately $12 million could be hidden from stockholders.

8. THE AUDIT

On the surface and from the auditors' view, Brightpoint's insurance policy had been in effect for six months prior to the close of 1998 fiscal period, and the policy provided up to $15 million of coverage for the UK loss. The three-year policy was written to require monthly premium payments. In actuality, no monthly payments were paid as the monthly premiums were prepaid. Consequently, the sham transaction in reality was one where Brightpoint paid AIG $15 million, and then AIG made a "payment" to Brightpoint for its loss. Brightpoint simply made a deposit to AIG and then received it back. AIG received an upfront fee of over $300,000 for its service. AIG and Brightpoint conspired to make the accounting documentation follow GAAP and consequently showing the insurance payment as a reduction of the trading loss. The payout from the retroactive policy was used to reduce the UK loss by close to $12 million.

Delaney and Harcharik engaged in a number of steps with AIG to successfully fool Brightpoint's auditors and stockholders regarding the true extent of the loss in financial statements prepared for the years 1999 through 2003. The first step they took was to develop documentation from AIG, and with AIG's cooperation, showing that although recoveries were not certain they were *highly probable*. Highly probable is the GAAP term that is required to consider the receivable on the policy as offset against the trading loss.[23] Other documentation included a letter of credit for $7.5 million from AIG, which was not needed but was useful in documenting GAAP requirements for the auditors. In actuality, there was no credit granted by AIG nor did AIG take any financial risk under the arrangement. Accounting guidelines also require that the policy must also transfer some of the risk of loss from the insured to the insurance provider.[24] If these two conditions are not met, payments to the insurer are considered deposits and payments to the insured are returns of deposits, not reimbursements for insurance losses.

In order to further confuse Brightpoint's auditors, the sham payments to AIG were supposedly made for the purchase of two types of insurance intermingled within the one insurance policy. One portion of the policy provided no exclusions and wide coverage for losses of up to $15 million. The second portion of the policy had a $15 million per loss limit along with a number of collection exclusions and restrictions. The second portion of the policy, which would never be used, was set

[23] Financial Accounting Standards Board Statement No. 5, *Accounting for Contingencies* (March 1975), ¶44, *Payments to Insurance Companies That May Not Involve Transfer of Risk*. Financial Accounting Standards Board, Norwalk, CT.

[24] Financial Accounting Standards Board Statement No. 5, *Accounting for Contingencies* (March 1975), ¶45, *Payments to Insurance Companies That May Not Involve Transfer of Risk*. Financial Accounting Standards Board, Norwalk, CT.

up to further the appearance of a risk transfer to the insurer as required under Financial Accounting Standards Board Statement No. 5. Brightpoint's sham advance "premium" payments for the contract covered both portions of the policy; thus making it difficult to determine the portion of the payment that should be allocated to each portion of the policy.

The first portion of the policy was the only reason for negotiating the policy, i.e., a return of the $15 million. The $15 million deposit with AIG was accounted for by Brightpoint as insurance premium payment in 1998 and loss recoveries receivable in order to reduce the 1998 loss. To further make the policy palpable to the auditors and less likely to be considered a deposit, there was no stipulation in the contract for a premium reimbursement for not making claims under the policy. The auditor's issued a "clean" opinion on Brightpoint's 1998 financial statements.

9. THE FRAUD EXAMINATION

Under subpoena pressure and a primarily investigation from the SEC in 2002 (see: Administrative Proceeding File No. 3-11251, In the matter of Brightpoint, Inc. Respondent), the "fraud examination" was begun by Brightpoint's auditors to determine what had occurred. After conducting a transaction-based fraud examination, Brightpoint's auditors required a restatement of Brightpoint's financial statements in 2001, and a second restatement in 2002. The first restatement required the entire $15.3 million paid to AIG be recognized as expense in the fourth quarter of 1998. The second restatement in 2002 required the disclosure of the deposit nature of the "premiums," essentially requiring the entire 1998 loss be recognized in the restated financial statements. The fraud examination conducted by the auditors was a transaction-based investigation to uncover the nature of the fraud and specifically related to the one event.

10. THE FORENSIC AUDIT

Fraud examinations can be part of a forensic audit or conducted separately. In the Brightpoint case, the fraud examination was not part of a forensic audit; therefore, no proactive forensic accounting procedures had been performed prior to the start of the fraud examination instituted by the auditors. Yet, forensic practices could have been used to curtail and identify the Brightpoint fraud. Forensic audit practices are expected to follow those principles that will best uncover the true economic risks occurring in a company. These methods are expected to begin before there is any hint of financial malfeasance in the organization and to be successful they must be continuous in nature.[25] Unlike the financial audit or the fraud examination that is performed under PCAOB or SAS guidelines, there is no

[25] The guide, *Managing the Risk of Fraud: A Practical Guide* (Institute of Internal Auditors 2008) outlines the procedures that should be followed in a fraud risk management programs. The Guide describes proactive approaches and continuous monitoring as important characteristics of a company's fraud risk management program.

book of rules for the forensic accountant to follow. Forensic practices must proceed in the manner that can best detect, stop, and collect evidence about fraud or unethical activities.

Prior to the start of the fraud examination by the auditors, internal controls within AIG and Brightpoint had been overridden by high-level executives in both companies; thus fooling the auditors. In this case, internal controls did not have any effect on preventing the fraud due to the managerial authority held by the co-conspirators. According to official documents, the fraud was unraveled when the SEC's staff issued a subpoena to the Brightpoint's auditors. With the knowledge that AIG-Brightpoint transactions were under investigation by the SEC, the co-conspirators attempted to hide their business transactions.

If forensic auditing had been used, the first step would be to conduct a review of Brightpoint's business culture. The result of such a review determines the level of monitoring that continuously occurs within Brightpoint. Such base-level monitoring would increase as targeted events occur within an organization. One such targeted event is the disposal of a business segment. Figure 2 illustrates the possible organizational relationship that could have been implemented between Brightpoint and a forensic service firm. The firm providing forensic auditing services should be completely independent from Brightpoint, and its employees should not perform their duties within any of Brightpoint's physical facilities. The forensic services firm's communication with Brightpoint is with selected members of Brightpoint's Board of Directors. Communications are limited to prevent any details about an investigation from be circulated among top-level managers and possible fraud conspirators. The forensic firm should not have any direct contact with individual executives at Brightpoint to prevent these managers from having any detailed knowledge about the forensic firm's monitoring and investigation activities.

With Brightpoint, digital monitoring would have been heightened with the forthcoming disposal of the UK division. The result would have been increased logging by digital forensic investigators of electronic data including e-mail traffic.[26] In the actual case, only with subpoena power was the SEC able to collect the following two e-mails from Delaney sent to Harcharik:[27]

---

[26] It would be expected that thousands of e-mails would need to be sorted through in order to find suspicious e-mails that attract the attention of the digital forensic investigators and members of the forensic fraud team. The preliminary review is automated. For example, the term “destroyed” in the second Delaney e-mail would result in the e-mail being logged and set aside for further reviewed by a forensic investigator. Such a review would involve an analysis of cross linked messages related to this e-mail.

[27] Securities Act of 1933, Release No. 8284, September 11, 2003; Securities Exchange Act of 1934, Release No. 48474, September 11, 2003; Accounting and Auditing Enforcement, Release No. 1854, September 11, 2003; and Administrative Proceeding File No. 3-11251. *In the Matter of Brightpoint, Inc., Respondent*. Order Instituting

"I need to support for [the Auditors] the recording of an insurance receivable related to the losses in the UK (in the amount of $12MM--Whoa)"

"The binder you signed (I looked at it again) has January 6, 1999 (in one case 1998) all over it. This is not good and that copy must be destroyed and [sic] with an August date executed."

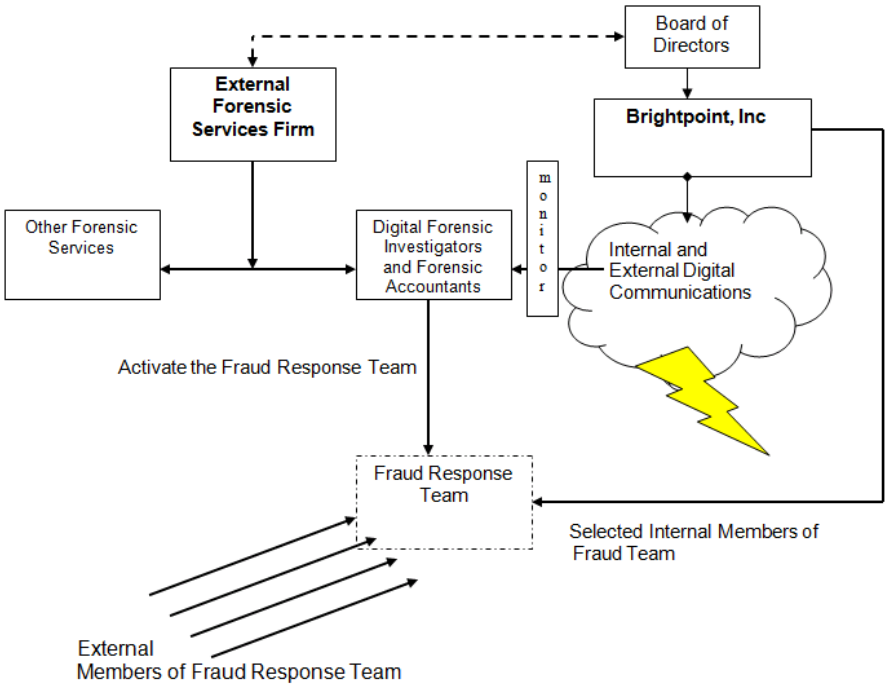

Figure 2. Forensic Services Firm Hierarchy with Brightpoint

Cease-and-Desist Proceedings, Making Findings, and Imposing a Cease-and-Desist Order Pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934 as to Brightpoint, Inc.

Unlike a financial audit, forensic auditing is not a periodic event. It is an ongoing process. Under a forensic audit, digital communications and documentation is independently and continuously reviewed by digital forensic investigators to identify any suspicious activity. Figure 2 illustrates the role digital forensic investigators play in a forensic audit of Brightpoint. Electronic data is collected from the company's LAN and includes e-mails or employee website activity used to identify potential fraudulent activity. Under such reviews, the previous two e-mails would have red-flagged the executive's activities.[28] At that point, selected members of a fraud response team would meet in emergency session to mitigate the fallout and damages to the company from the fraud. At a minimum, such a fraud response team should be composed of a chief investigator, external auditor, external attorney, internal company attorney, human resources officer, forensic accountant, public relations consultant, and several digital forensic investigators. Digital investigators along with the forensic accountants are responsible for convening the entire fraud response team when fraudulent activities are detected, such as the e-mails from Delaney.[29]

If forensic tools and practices had been used in this case, they would include the logged e-mails of all top company executives.[30] The level of e-mail privacy needs to be inversely related to the organizational authority of company managers because high-level managers have the ability to override traditional internal controls with relative ease.

11. CONCLUSION

The argument being made here is that it is not unreasonable to consider alternatives such as forensic audits to help provide stakeholders with assurances about the economic risks a company is facing. Such a step is especially important as the U.S. changes from a GAAP system strongly based on rules to one based on accounting principles.

---

[28] The reviews of electronic company documents go beyond the collection of e-mails. As the vast majority of business activities create an electronic footprint, the review of these business events allows insights into financial incidents that are otherwise unavailable. Under electronic monitoring, logs are collected and analyzed to provide information about the approval process for new vendors or claims for returned goods, for example. As a consequence, electronic authorizations can be immediately compared with the IP address on computers (or other devices) making the authorization with the IP address on computers pre-approved to make these changes. Further, funding authorizations can be evaluated for any dollar amount not just those above threshold spending levels.

[29] Under a forensic audit engagement, it is probable the activities of the co-conspirators would have been uncovered before these two e-mails were sent.

[30] In the United States, but not every other country, a company's property rights preempt an employee's privacy rights. An employer exercises a high level of control over an employees in the workplace based on the employment agreement whereby the employee is not required to work for the employer, but once a position of employment is accepted then the employee must follow workplace rules (Eltis 2003).

Forensics and fraud practices have commonalities of interest. Both approaches must apply a mindset that does not easily fit within the audit environment. But, fraud is a more specific and limited examination. Forensics is broader, and it fits into a principles-based environment. The Global Report closes with the call, "Let us begin the conversation" (Global Public Policy Symposium 2006). We hope this article adds to the necessary dialogue.

12. REFERENCES

Abernethy M. 2004. On the day of reckoning, *Charter*, (August) <http://www.allbusiness.com/accounting-reporting/forensic-accounting/1002194-1.html>. Accessed January 19, 2008

Brewster, M. 2003. *Unaccountable: How the Accounting Profession Forfeited a Public Trust.* John Wiley and Sons (

Brooks, D., Goldman, M. and Lanza, R. 2007. *Buyer's Guide to Audit, Anti-Fraud, and Assurance Software*. Ekaros Analytical, Inc. (Vancouver, Canada)

Eltis, K. 2003. The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Caselaw in Canada and Israel: Should Others Follow Suit? *Comparative Labor Law & Policy Journal* Vol. 24 (3): 487-524.

Global Public Policy Symposium. 2006. *Global Capital Markets and the Global Economy: A Vision from the CEO's of the International Audit Networks*. (November) <http://www.globalpublicpolicysymposium.com> Accessed January 19, 2008.

Global Public Policy Symposium. 2008. *Principles-Based Accounting Standards*. (January) New York. <http://www.globalpublicpolicysymposium.com/documents.htm> Accessed January 19, 2008.

Institute of Internal Auditors. 2008. *Managing the Business Risk of Fraud: A Practical Guide.* David A. Richards, Project Manager. Published by the Institute of Internal Auditors, American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners.

Kahan, S. 2006. Sherlock Holmes Enters Accounting. *WebCPA: Tools and Resources for the Electronic Accountant*, (May 1) <http://www.webcpa.com/article.cfm?articleid=20019&pg=ros>. Accessed March 20, 2009.

Michaud, D., Dutton, C. and Magaram, K. 2006. Empowering Board Audit Committees: Electronic Discovery to Facilitate Corporate Fraud Detection, Brown University Corporate Governance Program. Working Paper <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=896004> Accessed May 8, 2008.

May, G. 1937. Principles of Accounting, *Journal of Accountancy*, 64, 423-425.

May, G. 1950. Truth and Usefulness in Accounting," *Journal of Accountancy*, 89, 387.

Public Company Accounting Oversight Board (a). 2007. *Observations on Auditors' Implementation of PCAOB Standards Relating to Auditors' Responsibilities with Respect to Fraud.* PCAOB Release No. 2007-001. (Washington, D.C).

Public Company Accounting Oversight Board (b). 2007. *Panel Discussion: Forensic Audit Procedures.* PCAOB Standing Advisory Group Meeting. February 22. (Washington, D.C).

Shortridge, R. and Myring, R. 2004. Defining principles-based accounting standards. *The CPA Journal*, 74, (August) 34-37

Smith, G. and Crumbley, L. 2009. How Divergent are Pedagogical Views Toward the Fraud/Forensic Accounting Curriculum? *Global Perspectives in Accounting Education* Vol. 6 (2009) 1-24. <http://gpae.bryant.edu/~gpae/content.htm> Accessed March 20, 2009.

Smith, G. 2005. Computer forensics: Helping to Achieve the Auditor's Fraud Mission?" *Journal of Forensic Accounting, Auditing, Fraud & Taxation* Vol. 4 (1) 119-134.

Tinker, T. 1986. *Social Accounting for Corporations: Private Enterprise versus the Public Interest.* Markus Wiener Publishing, Inc. (New York, NY).

Wagner, M. and Frank, P. 1986. *Management Advisory Services Technical Consulting Practice Aid 7: Litigation Services*. American Institute of Certified Public Accountants (New York:, NY).