THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 1 | Number 4 Article 1

2006

A Curriculum for Teaching Information Technology Investigative Techniques for Auditors

Grover S. Kearns

College of Business University of South Florida, St. Petersburg

Follow this and additional works at: http://commons.erau.edu/jdfsl

 Part of the Computer Law Commons, and the Information Security Commons

Recommended Citation

Kearns, Grover S. (2006) "A Curriculum for Teaching Information Technology Investigative Techniques for Auditors," *Journal of Digital Forensics, Security and Law*: Vol. 1 : No. 4 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2006.1011
Available at: http://commons.erau.edu/jdfsl/vol1/iss4/1

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE Aeronautical University SCHOLARLY COMMONS

(c)ADFSL

A Curriculum for Teaching Information Technology Investigative Techniques for Auditors

Grover S. Kearns
College of Business
University of South Florida St. Petersburg
St. Petersburg, Florida 33701-5016 USA
gkearns@stpt.usf.edu

ABSTRACT

Recent prosecutions of highly publicized white-collar crimes combined with public outrage have resulted in heightened regulation of financial reporting and greater emphasis on systems of internal control. Because both white-collar and cybercrimes are usually perpetrated through computers, internal and external auditors' knowledge of information technology (IT) is now more vital than ever. However, preserving digital evidence and investigative techniques, which can be essential to fraud examinations, are not skills frequently taught in accounting programs and instruction in the use of computer assisted auditing tools and techniques – applications that might uncover fraudulent activity – is limited. Only a few university-level accounting classes provide instruction in IT investigative techniques. This paper explains why such a course would be beneficial to the program, the college, and the student. Additionally, it presents a proposed curriculum and suggests useful resources for the instructor and student.

Keywords: computer forensics, auditors, IT investigative techniques, IT audits, cybercrime, accounting curriculum development

1. INTRODUCTION

Escalation of computer related crimes has increased the importance of information technology (IT) forensics knowledge to accountants and to auditors particularly. Two studies were early harbingers of workplace fraud. In 1987, the Committee of Sponsoring Organizations (COSO) issued the Report of the National Commission on Fraudulent Financial Reporting. In a 1999 follow-up study that looked at fraudulent activities for public companies during the period 1987 to 1997, the report found 300 cases of financial statement fraud perpetrated in 200 randomly selected publicly traded companies. Chief offenses were improper revenue recognition, overstatement of assets, and understatement of expenses and liabilities (COSO 1999; Beasley et al. 1999). Evidence for many of these frauds was in the form of digital data residing on computers and storage devices. Because electronic evidence is highly volatile, preservation of the evidence required knowledgeable experts who could access

it in a timely manner.

In the 2004 Fraud Survey by big four accounting firm KPMG, 55 percent of respondents felt that financial fraud could have been detected and prevented if accountants had more training with identification of "red flags." A surprisingly large 73 percent of respondents stated that the management of fraud risk within their organization was "not well defined."

In 2002, the National Association of Certified Fraud Examiners (NACFE) issued a report, known as the Wells Report, based on a study of 663 fraud cases. The results were compared to a previous 1996 study by the NACFE. Between 1996 and 2002, the cost of occupational fraud was estimated to have increased from $400 billion to $600 billion. The three primary methods of committing fraud were identified as asset misappropriation, corruption, and fraudulent financial statements. Any of the categories in the Wells Report could be committed using IT and the report cited increased reliance on computers as a possible source of increased fraud (Hunton et al. 2004).

The new millennium issued in new regulations affecting the role of IT in auditing. In 2001, Statement of Auditing Standards (SAS) No. 94 recognized the effect IT had on internal control and the scope of the audit. In 2002, SAS No. 99 extended the auditor's role in uncovering fraud in financial statements. The Sarbanes-Oxley Act of 2002 (SOX) – enacted in the wake of major financial reporting frauds and executive misconduct – is now common knowledge for accounting students. Together, these regulations increased the importance of accountants' IT knowledge. However, at least one study indicates that post-SOX audit firms may continue to misstate audit opinions in order to please management (Chaney, Jeter, and Shaw 2003).

The main goal of IT investigative techniques is to determine if a compromise has occurred. If so, it is imperative, to the extent possible, that the first responder preserves all evidence and document the scene. Digital evidence can disappear before management is alerted and a specialist can arrive. Because audits involve investigation of internal controls and detailed analysis of transactions, either the internal or external auditor might be the first to recognize a fraud has occurred or that a computer or network has been compromised. Knowledge of how to freeze the scene and an understanding of how digital evidence will be subsequently processed and maintained is the subject of IT investigative techniques. Accordingly, the purpose of this paper is to (1) examine the need for internal and external auditors' knowledge of IT investigative techniques; (2) show how forensics can increase the organization's ability to combat corporate crime; and (3) present a template for modeling educational curriculum to train forensic auditors.

2. FORCES DRIVING NEED FOR IT INVESTIGATIVE TECHNIQUES COURSE

2.1 Increased Business Reliance on IT

Business reliance on IT is well documented (Hunton et al. 2004; Posthumusa and Solms 2005) and is reflected in more recent Statements on Auditing Standards (SAS) and control documents such as COBIT and the IT control objectives for Sarbanes-Oxley.

SAS 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*, increased the auditor's focus on IT by noting that, where a significant portion of accounting data is in electronic form, then the auditor should gather evidence about the effectiveness of controls over the design and operation of information systems. Further, SAS 94 states that proper examination of IT controls may require the auditor to develop specialized skills.

SAS 99, *Consideration of Fraud in a Financial Statement Audit*, proactively addressed increased reports of fraud in the workplace by implementing audit procedures to uncover fraudulent acts by management and employees. This had two impacts on the auditor's role. First, it extended the need for forensic skills to properly analyze large amounts of data. Second, it removed the concept of materiality: all acts of fraud were important regardless of the impact on the financial statements.

COSO, the Committee of Sponsoring Organizations of the Treadway Commission, was formed in 1985 to study the factors underlying workplace fraud. Two important studies followed. A 1987 study reported on the enforcement actions of the SEC for the period 1981 to 1986. A follow-up study in 1999 reported on fraudulent financial reporting for the period 1987 to 1997. These studies gave impetus to the development of both SAS 94 and 99 (COSO 1987, 1999).

COBIT, Control Objectives for Information and related Technology, is a framework for information security created by the Information Systems Audit and Control Association, and the IT Governance Institute. As an IT governance framework, COBIT plays an important role in the IT audit function (Hawkins et al. 2003).

Increased reliance has resulted in a tightening of security measures which is the responsibility of the IT function but important to accountants for internal control. Security measures are highly proactive and breaches are often treated immediately to avoid business interruption and counter any malicious threats. Security measures, however, may not detect acts of fraud that can surface during an audit. In order to collect digital evidence and identify the suspect, it may be necessary to take immediate action.

Handling digital evidence requires training. The Group of Eight (G8) – which consists of the U.S., Japan, Germany, France, the U.K., Italy, Canada and Russia – have issued guidelines for the collection of digital evidence and stated that standard forensic principles must be applied and that people who initially handle original digital evidence should be trained for that purpose (G8 Online).

IT investigative training can be expensive. For example, one vendor, Technology Pathways, charges $2,500 for a three day workshop on a single forensics tool (source: http://www.techpathways.com/). While accountants may not become highly skilled in computer forensics, businesses need an internal staff who are sufficiently skilled in recognizing computer-related crimes and who possess sufficient skills as first responders. In the words of Peter Sommer of the London School of Economics, "IT-dependent companies need to understand that police can't be expected to investigate crimes and recover assets if reasonable precautions haven't been taken" (Sommer 2004).

2.2 Increase in Computer-Based Risks

Three categories of computer associated risks are of interest to accountants and auditors. First is corporate fraud aimed at manipulating the financial statements (financial reporting fraud) in order to improve the bottom line. This type of fraud directly benefits the business, but it is often perpetrated to indirectly enrich senior managers. Second is the fraud that is committed by employees and/or outsiders for self-enrichment. This often requires access to computer programs or files. It may involve collusion between employees and outsiders as is the case with vendor kickback schemes. Third is the risk of malicious intrusion by either insiders or outsiders such as by disgruntled employees and hackers.

The first two categories are documented in the COSO study and represent the use of computers to commit a criminal act. The third category represents crimes against computers or networks (e.g., computer crimes) and has been documented in a number of reports including the FBI 2005 computer crime survey. In the survey, the FBI states that 90 percent of the surveyed organizations have experienced a computer attack, 20 percent have experienced 20 or more attacks, and 64 percent have suffered a financial loss (FBI 2005). The Data Genetics International 2003 study on corporate crime revealed intellectual property theft and employee fraud to be the prime targets of corporate investigations. In several cases valuable evidence was lost or destroyed because suspects had been inadvertently alerted about the investigation and/or unqualified persons had handled the computers prior to forensics processing (Wilding 2003).

According to the Association of Certified Fraud Examiners, cybercrimes are increasing in number and intensity (2002). There has been a marked increase in malicious code attacks with intent to destroy or capture business data and

phishing and pharming attacks are becoming highly sophisticated increasing the likelihood of loss (Websense 2006). Well known companies such as Marriott, Choicepoint, and Bank of America have suffered the loss of confidential customer information and data breaches.

2.3 Impact of Sarbanes-Oxley on IT

SOX has provided added impetus for senior management of publicly traded companies to insure the existence and adequacy of a system of internal controls. Because business systems are almost totally computerized, audit of IT controls is now essential to a financial statement audit. Any fraud perpetrated is most likely to occur on a computer or network and surveys have shown that most financial frauds are perpetrated by insiders with access to information systems (Hunton et al. 2004).

It is estimated that 93 percent of all business documents are in electronic form and only 30 percent are ever printed (Lange 2003). Because the preponderance of information that is the basis for management attestation is stored in information systems, SOX Section 404 increases the role and importance of IT audits. Thus, senior management must increase emphasis on IT governance in order to provide for internal control over information systems and assets and meet SOX guidelines (Worthen 2003; Logan 2004). Consequently, auditors will require more advanced knowledge of information systems and technologies.

Problems associated with preservation of electronic evidence are well documented. Digital data does not have the same legal status as paper evidence (Giordano 2004). Inappropriate recovery and handling of electronic data can result in the inadmissibility of the evidence in court as in the $2.75 million judgment against the defendant in *United States v. Phillip Morris* (Anonymous 2005). Computer literate attorneys are now knowledgeable of the problems attendant with electronic discovery and will quickly challenge the recovery methods and chain-of-custody in these cases (Anderson 2006). Thus, specialists in computer forensics are more likely to recover data in a manner that supports admissibility in legal proceedings (Smith 2005).

3. STATUS OF IT INVESTIGATIVE TECHNIQUES IN ACCOUNTING PROGRAMS

Accounting programs may be outdated, not reflecting major changes in the business environment and, as a result, students are not equipped with the skills they will actually need in practice (Gabbin 2002). One survey found that accounting students lacked the requisite IT knowledge to perform their career positions (Ahmed 2003).

Buckoff and Schrader (2000) found that a forensic accounting course would benefit the accounting program, the accounting students, and the employers. In their study, they noted that most fraud courses do not address the forensics

issues that are now important to accountants and especially to auditors. Forensic accountants need specific instruction in investigative auditing techniques (Crumbley et al. 2005). Courses in fraud and forensic accounting are usually offered only at the graduate level and may represent a special track or elective course. Moreover, these courses can omit important IT investigative techniques that relate to the collection and protection of evidentiary matter and the more technical IT topics. In a discussion memo, the AICPA has recognized the need for more advanced skills by stating "a new certification designed to test and certify individuals in forensic accounting technical procedures may validate and add to the skill sets professional forensic accountants currently obtain" (AICPA 2006).

In large accounting departments at U.S. schools, 84 percent offer an Accounting Information Systems (AIS) course while only 67 percent of medium size departments and 44 percent of small accounting department offer AIS (O'Donnell and Moore 2005). The percentage of schools in which the AIS course is required is even lower. Thus, not all accounting students have instruction in AIS which introduces information technology control issues.

Busing et al. (2005/2006) found that, because computer related crimes will continue to grow, more universities are preparing courses specifically for computer forensics. The technical prerequisites for such courses, however, could vary from familiarity with basic IT knowledge to extensive computer sciences knowledge. Also, computer forensics includes discussion of illegal activities such as child pornography and a focus on Unix systems which are not subjects of great importance to accountants and auditors. For this reason, a course specifically designed for auditors with an accounting background and limited IT knowledge would be beneficial. A small number of colleges of business now offer some course of IT investigative instruction as part of a forensics accounting program.

3.1 Professional Certifications

There are a number of professional certifications in the area of fraud and forensics accounting. Instruction in IT investigative techniques would help prepare accounting students to meet the requirements for the certifications. Because the demand for accountants with specialized knowledge in this area is increasing, the certification can improve the student's career opportunities. Two popular examples are the Certified Forensic Accountant (Cr.FA) and the Certified Fraud Examiner (CFE). The American College of Forensic Examiners, a 15,000 member body, first offered the Cr.FA designation in 2001 and requires two exams. Persons holding an accounting certificate are only required to take the second exam. The Association of Certified Fraud Examiners, a 32,000 member body, was established in 1988 and its membership includes accountants, lawyers, detectives, college faculty, and students. The exam for the CFE focuses on fraud examination and

investigation (Crumbley et al. 2005).

Ahmed (2003) identifies a "hybrid accountant" as one who blends both accounting and IT skills. These certifications combined with instruction in IT investigative techniques will help to elevate the student to a "hybrid auditor" – one who blends forensic accounting skills with IT skills.

4. TEACHING CONSIDERATIONS

4.1 Teaching Style

Teaching will be more effective if the instruction parallels the students' learning styles. Research has shown that about 65 percent of business students are extraverts. Extraverts must participate actively in order to learn. It might be expected that accounting students would be slightly less so but still remain extraverted (Dudley et al. 2003).

Of the many learning style models devised, the Felder-Silverman model has been found to be appropriate for the sciences. Because accounting students are more oriented to structured, quantitative techniques and the class focus is technical, this model is appropriate. The model classifies students into five dichotomous classes: sensing or intuitive learners, visual or verbal learners, inductive or deductive learners, active or reflective learners, and sequential or global learners (Felder 1996). Recent research of business statistics students shows a preference for sensing, visual, active, and sequential learning styles (Naik 2003).

Sensing learners, the majority of students, would need for problems to be presented and explained step-by-step in a linear fashion either on a white board or overhead projector. Examples of how applications would be applied in the real world would be appropriate. Visual and active learners would both benefit from hands-on activities while active learners would need hands-on activities and would enjoy group assignments. By reviewing previous material and explaining how it relates to the new material, the instructor will assist the sequential learners. These students can be expected to do well on case studies.

This research showed only a small number of the students to be intuitive, verbal, reflective, or global learners. Thus, classroom instruction styles should be directed towards the sensing, visual, active, and sequential learning styles.

4.2 The Classroom

Because of the technical nature, the class would ideally be held in a computer lab. At minimum, ready access to a lab should be available to provide for in-class exercises using the investigative software. Labs also assist in on-line tutorials that are often provided with textbooks and for on-line search of cases and related materials.

Additionally, the classroom should be equipped with an overhead projector for

displaying PowerPoint slides and to illustrate use of investigative software applications. An overhead projector, such as an Elmo, and a white board would also be important resources.

Security reasons and licensing issues may limit the number of computers to which certain software applications can be loaded. Sometimes vendors will make demo copies of software products available for in-class demonstration. If possible, the instructor may wish to create one or more forensics workstations for special assignments that require special operating systems.

4.3 Other Teaching Resources and Techniques

Because a wide disparity in technical knowledge among accounting students can be expected, the more knowledgeable students can be teamed with students who possess limited IT skills in order to quicken the learning curve. This can be facilitated using the in-class survey and assigning group members in order to balance existing knowledge. Students should take responsibility for seeking out information. The Internet offers excellent resources (see Table 1).

Textbooks at libraries covering technical subjects are often outdated. Texts relating to computer forensics and accounting forensics should be placed on library reserve for students. Some of these are listed in the references section of this paper. If research papers are assigned, these will provide a valuable resource – one that is not on the Internet.

Professional associations and local accounting firms are good sources for outside speakers. Persons with practical knowledge are highly effective in relating real-world cases and increasing student interest. Opportunities for practitioner interaction with students in the classroom, on field trips, or by internships can also be used to motivate students and bring a sense of reality to the material (Gabbin 2002).

Resources should be made available online using either Blackboard, WebCT, or the instructor's own web site. Links to relevant materials can be provided. A partial list of related links is shown in Table 1.

Table 1. A Partial List of Web Sites for Reference and Class Assignments

Site	Web Site URL	Information
COSO Model	http://www.coso.org/	The COSO Model
COBIT Control Model	http://www.isaca.org/	The COBIT Model
Sarbanes-Oxley	http://www.sarbanes-oxley.com/	The SOX site
IT Governance Institute	http://www.itgi.org/	IT Control Objectives for Sarbanes-Oxley
Computer Forensics Resources	http://www.forensics.nl/tools	Links to related sites and white papers
IT Audit	http://www.theiia.org/ITAudit/index.cfm?act=itaudit.archive&fid=325	IT resource for auditors
Timberline Technologies	http://www.timberlinetechnologies.com/products/forensics.html	List of forensics software applications with related links
G8 Online	http://www.g8online.org/2005/english/index.html	International portal
Networkworld	http://www.networkworld.com/supp/2004/cybercrime/112904cybersecurity.html	Security issues, summary of surveys, recent attacks
Websense	http://www.websense.com/global/en/	Security reports
Auditnet	http://www.auditnet.org/audsoft.htm	Audit portal with security software information
Wickapedia	http://wickapedia.net/	Knowledge center
Howstuffworks	http://computer.howstuffworks.com/	Explanations of computer terms and procedures

5. PROPOSED COURSE CONTENT

The proposed course content is based on a three-hour semester graduate class. This assumes approximately 45 hours of classroom instruction although some of the technical matter could be made available electronically via Blackboard, WebCT, or the instructor's own web site. The suggested curriculum could be modified for undergraduate courses or quarter hour systems. Course objectives that could be included on the class syllabus are shown in Table 2. Proposed course content is shown in Table 3. Content in Table 3 is rated for both the expected audit and IT knowledge levels where 1 reflects a low level and 3 a high level of knowledge. Content will vary according to the specific program goals that the course supports and the expected audit and IT abilities of the

students. Using Table 3, content can be selected that matches both the course objectives and students' abilities.

5.1 Non-Technical Course Content

Non-technical content will depend on the context of the course. If the course is offered as part of a program that includes courses in fraud detection and forensic accounting, then less emphasis will be given to topics that overlap those courses. However, if the course is an elective and students may not have received instruction in fraud examination and forensic accounting, then the course outline should include such topics from those areas. In the first case, knowledge could be assumed and a brief review would suffice. In the latter case, attention to financial statement fraud examination and detection methods would be necessary.

Course focus should be on cyber crime and white collar crime, legal issues, crime detection, and information assurance. Information assurance and authentication is vital in order that auditors protect the integrity of digital evidence (Duerr et al. 2004). Attention must also be given to the expanded role of IT controls that emanate from Sarbanes-Oxley. A review of the COSO and COBIT models and the IT control objectives for Sarbanes-Oxley would be appropriate during the first two class meetings. Online assignments can be given using information available at the web sites shown in Table 1. Assignments could include topics such as the identification of IT-related risks, incident response techniques, first responder strategies and protocols, and the use of CAATs. If the course is an elective within an overall program that does not include other fraud or forensics classes, then topics must be more general. Within a program that focuses on fraud and forensics, the topics should be selected to extend knowledge in the more technical areas of forensics with special attention on disk imaging and analysis using models such as ACL.

Table 2. Suggested Course Objectives for IT Investigative Techniques

At the end of the course students should have a basic understanding of:
➢ How computer related crimes impact the audit function
➢ How knowledge of IT investigative techniques can enhance career opportunities
➢ Information technology control objectives
➢ How to assess risks related to IT networks and telecommunications
➢ How to assess risks related to electronic commerce
➢ The use of CAATs including specific knowledge of tools such as ACL
➢ Hardware and software related to computer forensics including disk data structures
➢ Computer forensic tools including bit-stream imaging tools
➢ How to freeze the scene and begin a chain-of-custody for electronic evidence
➢ Legal and ethical issues regarding computer crime and IT controls

Table 3. Suggested Topics and Estimated Knowledge, Skills and Abilities for an IT Investigative Techniques Course

Topic	Audit KSA	IT KSA	Description
Information Technology and Internal Control	2	1	Overview of internal control objectives (SAS 94, SAS 99), Sarbanes-Oxley 2002, IT control objectives, COSO and COBIT models, IT control objectives for SOX, Benefits of the forensics methodology, Digital forensics careers and certifications
The IT Function	1	1	Structure of the IT function, Systems development, General and application controls, Segregation of incompatible IT functions, Distributed processing, Disaster recovery
Hardware and Software	1	3	Operating systems, Compilers and interpreters, Disk structures, FAT and NTFS, RAM, CPU
Data Structures	1	3	Relational and hierarchical databases, Schemas, Access controls, Sequential files, ISAM, Random access files, Anomalies
Networks, Internet, and E-Commerce	1	3	Network topologies, WAN/LAN, Gateways and routers, TCP/IP, Servers, EFT, EDI and X.12, HTML, XML, XBRL, Wireless, 802.11n, Transaction logs, Log file analyzers, Intrusion detection
Data encryption	1	3	Encryption, Hash algorithms, Secret and public key systems, Digital signatures and certificates, Certification authorities, Veri-sign, TrustE, Integrity, Authentication, Nonrepudiation, Steganography, RSA, 3DES, MD5, PGP, Blowfish
Computer-Assisted Audit Tools and Techniques	3	3	CAATs and generalized audit software, Audit trail controls, Output controls, Validation checks, Check digits, File/record interrogation, Input/Processing/Output controls, Test data method, Integrated test facility, GAS, ACL, Embedded audit modules
ACL Instruction	2	2	Assignments to identify anomalies that could indicate fraudulent activities
Cyber Crime, Computers and the Auditor	2	2	Cyber crime and related laws, Accounting and auditing standards affecting the auditors responsibility and guidelines for IT related audits, The digital crime scene

Table 3. Suggested Topics and Estimated Knowledge, Skills and Abilities for an IT Investigative Techniques Course (cont.)

Topic	Audit KSA	IT KSA	Description
Digital Evidence Seizure	1	1	G8 guidelines for handling digital evidence, Digital media, Securing evidence at the scene, Processing and handling evidence, Documenting and cataloging evidence, Preserving evidence, Cyclical redundancy checksum, MD5 checksum
Recovery of Digital Data (Optional)	2	3	Hard disk file structure, Free space, File slack, RAM slack, Recovering deleted and hidden files, Evidentiary data and chain of custody, Daubert versus Frye compliance
Forensic and Analytical Tools (Optional)	1	3	The forensics workstation, Imaging software (EnCase, Safeback, Norton Ghost, Snapback), Coroner's Toolkit, Digital Detective, Benford's Law, ACL
Information Assurance and Authentication	2	1	Authentication of digital evidence: integrity and non-repudiation, Access and physical controls
E-Mail	1	2	Mail protocols (POP, IMAP, SMTP), Examining e-mail headers andl server logs, Tracing an e-mail message
Becoming an Expert Witness (Optional)	2	1	Role of the expert witness, the expert as legal consultant, the expert as master and special master, Protection of work product, Criminal and civil litigation, Discovery, Subpoenas and warrants, The expert witness report, Malpractice
Legal Issues Affecting the IT Audit	2	1	Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Title 18 USC 2703 (f)

The majority of students will not develop the technical skills to actually process computer evidentiary matter. However, incident response techniques and accepted standards for handling evidentiary matter are vital to auditors who want to preserve digital evidence on a computer (Kruse and Heiser 2002). It is imperative that auditors know when to recognize the need for a computer forensics specialist, how to process a suspected fraud scene, and how to properly bag and tag computer hardware and software at the scene before a specialist arrives. Otherwise, auditors may unknowingly destroy critical information or lose it because they did not freeze the scene in a timely manner. Proper training can prevent the destruction of evidence and save money by

having employees perform certain investigative techniques such as documenting the scene.

5.2 Technical Course Content

While soft skills are highly important for progression into senior positions, research shows that technical skills are most important in the early career stages (Blanthorne et al. 2005). Technical content should be the major thrust for IT investigative techniques. At the graduate level, more foundation knowledge might be assumed but the instructor should survey the class for technical knowledge. A suggested survey form is shown in Appendix A.

Some students will already be familiar with computer assisted audit tools (CAATs). Several textbooks including the Hall and Singleton (2005) textbook and the Hunton et al. (2004) text book include the ACL software and accompanying exercises. This activity will appeal to most student's learning style and can be performed in-class or as an outside assignment. Although instruction is provided with the software, the instructor should take time to illustrate the basic steps of using the software on the overhead projector and allow students to work on a tutorial before making a specific assignment. This will appeal to students with a sensing learning style.

Because most students have difficulty retaining technical material and are likely to forget important instructions on incident handling under the stress of a real-world situation, the use of flow-diagrams that represent situational protocols is recommended. The Kruse and Heiser text on incident response presents an excellent set of diagrams for responding to various incidents including malware attacks and network probing (2002, pp. 337-349).

More technical textbooks contain computer forensics software. The Nelson et al. (2006) textbook contains various forensics tools. However, some of the tools require a workstation that has a Windows 98 or 95 operating system in order to use DOS commands. This is impractical for an entire lab but could be enabled on one or more separate forensic workstations. If this approach is taken, a DOS command manual should be made available to the class. An alternative would be to discuss these software applications and for the instructor to illustrate several on an overhead projector. The Vacca (2002) textbook includes a file recovery software, a binary file editor, the WinHex tool suite which can recover deleted or lost data from damaged hard drives, and a packet-sniffer program. These would be useful as reserve materials.

Some texts include educational or demo versions of software and some vendor web sites offer free demo copies of forensic software such as the X-Ways Forensics tool. For example, the Hall and Singleton text includes ACL software and a teaching tutorial that would be excellent for case assignments. The Nelson et al. text includes a limited version of EnCase plus access to DriveSpy and Image. Teaching software tools is time-consuming and must be

balanced with the students' future need for similar tools.

Although, in practice, actual teaching plans will depend upon specific programmatic goals, a sample teaching plan can assist educators in preparing for a first course. Appendix B presents a sample teaching plan based on a fifteen week semester plus final exam week. The plan includes three ACL cases that could be performed in-class.

5.3 The Hybrid Auditor

The goal of the IT investigative techniques course should be to elevate the student to the role of a hybrid auditor. It is not expected that students will possess a high level of both auditing and IT knowledge upon graduation. However, an introduction to the basics of investigative techniques will prepare the student to recognize the forensic tools and procedures available and allow for the future expansion of knowledge along both the accounting and IT investigative paths. Figure 1 presents the hybrid auditor matrix. Auditors who possess increased knowledge, skills, and abilities (KSAs) in IT can operate as IT auditors. Those with enhanced forensic accounting KSAs can server as forensic auditors. By blending both enhanced forensic and IT skills, the hybrid auditor emerges.

Students who lack technical skills and possess mainly soft skills will enter their careers as auditors and may be held back from further progression. IT students will possess high levels of IT skills but will possess no accounting skills. However, accountants who have developed both forensics and IT investigative knowledge may eventually move into the area of hybrid auditor. As such, they will be more valuable to the business and could be expected to have brighter career paths.

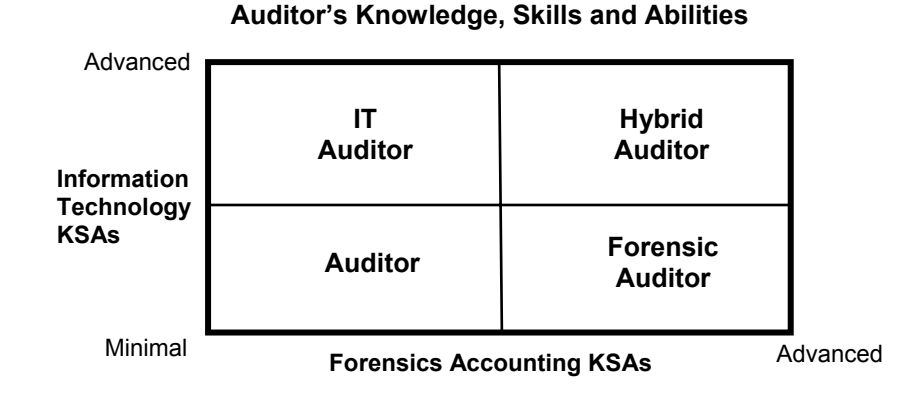

Figure 1. The Hybrid Auditor Matrix

6. CONCLUSIONS

This paper articulates the need for auditors to develop computer forensics knowledge. Because both internal and external auditors are in a position to detect signs of fraud and act as first responders and because electronic evidence can easily be corrupted, the hybrid auditor can serve a critical business need as coordinator of electronic evidence. During the initial stages, he or she can secure the scene and begin the chain-of-custody. During the investigation, the auditor can play a coordinating role with management, IT specialists, and law enforcement officials.

This paper makes several contributions. First, it supports a clear need for a forensics based course for auditors. There is a growing need for employees who are knowledgeable about handling digital evidence in a fraud case. Second, the paper discusses the current status for IT investigative techniques in accounting programs. Third, the paper outlines the curriculum for such a course. The list of topics is extensive and can be modified according to the particular accounting program in which the course will be offered. Finally, the paper suggests appropriate resources including textbooks, a study survey, and websites for this course of study. Programs and course instructors considering the introduction of this material into their own curriculum will benefit by having a guide for development. Future researchers will benefit by having a framework to evaluate and critique such courses.

For businesses that are IT-intensive, an IT investigative techniques course will assist in creating the hybrid auditor. This will advance fraud examination and increase the likelihood that fraudulent activities will be uncovered and digital evidence will be extracted using acceptable forensic standards.

7. REFERENCES

Ahmed, A. (2003), "The Level of IT/IS Skills in Accounting Programmes in British Universities," *Management Research News*, 26 (12): 20-58.

AICPA Discussion Memo (2006), Retrieved May 1, 2006 from http://72.14.207.104/search?q=cache:pTaB2z8CToQJ:www.theiia.org/iia/download.cfm%3Ffile%3D3975+AICPA+and+forensics+accounting&hl=en&gl=us&ct=clnk&cd=4.

Anderson, M.R. (2006), "Computer Evidence Processing," *New Technologies, Inc*., Retrieved April 20, 2006 from http://www.forensics-intl.com/art7.html.

Anonymous (2005), "Computer Forensic Investigations Require the Skills of Trained eDiscovery Specialists," eMag Solutions, Retrieved May 10, 2006 from http://www.emaglink.com/newsletter_archive/newsletter_December_2005.htm

Association of Certified Fraud Examiners, *2002 Report to the Nation: Occupational Fraud and Abuse*, View at www.cfenet.com/pdfs/2002RttN.pdf

Beasley, M.S., Carcello, J.V. and Hermanson, D.R. (1999), "COSO's New Fraud Study: What it Means for CPAs," Journal of Accountancy, 12-13.

Blanthorne, C., Bhamornsiri, S. and Guinn, R.E. (2005), "Are Technical Skills Still Important?" *The CPA Journal*, 75 (3): 64-67

Buckoff, T.A. and Schrader, R.W. (2000), "The Teaching of Forensic Accounting," Journal of Forensic Accounting, 1 (1): 135-146.

Busing, M.E., Null, J.D. and Forcht, K.A. (Winter 2005/2006), "Computer Forensics: The Modern Crime Fighting Tool," *The Journal of Computer Information Systems*, 46 (2): 115-119.

Cerullo, M. V. and Cerullo, M. J. (2003), "Impact of SAS No. 94 on Computer Audit Techniques," *Information Systems Control Journal*, 1: 1-5.

Chaney, P.K., Jeter, D.C. and Shaw, P. (2003), "The Impact on the Market for Audit Services of Aggressive Competition by Auditors," *Journal of Accounting and Public Policy*, 22 (6): 487-516.

COSO (1987), "The Report of the National Commission on Fraudulent Financial Reporting," *The Committee of Sponsoring Organizations*, Retrieved May 1, 2006 from www.coso.org/Publications.

COSO (1999), "Fraudulent Financial Reporting 1987–1997: An Analysis of U.S. Public Companies," *The Committee of Sponsoring Organizations*, Retrieved May 1, 2006 from www.coso.org/Publications.

Crumbley, D.L, Heitger, L.E. and Smith, G.S. (2005), *Forensic and Investigative Accounting, 2nd Ed.*, CCH Incorporated, Chicago, IL.

Dudley, S.C., Dudley, L.W. and Chandler, E.W. (2003), "Learning Styles Of Business Students." View at: http://www.swlearning.com/marketing/gitm/gitm4e08-21.html

Duerr, T.E., Beser, N.D. and Staisiunas, G.P. (2004), "Information Assurance Applied to Authentication of Digital Evidence," *Forensic Science Communications*, 6 (4).

FBI 2005 Computer Crime Survey (January 18, 2006), View at http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm

Felder, R.M. (1996), "Reaching the Second Tier: Learning and Teaching Styles in College Science Education," *Journal of College Science Teaching*, 23 (5): 286-290.

G8 Online, (2006), "An Online University Level Course About the G8 and its Annual Summit," Retrieved April 15, 2006 from http://www.g8online.org/2005/english/index.html.

Gabbin, A.L. (2002), "The Crisis in Accounting Education," *Journal of Accountancy*, 193 (4): 81-86.

Giordano, S.M. (2004), "Electronic Evidence and the Law," *Information Systems Frontiers*, 6 (2): 161-174.

Hall, J. and Singleton, T. (2005), *Information Technology Auditing and Assurance, 2nd Ed.*, Thomson South-Western, Mason, OH.

Hawkins, K.W., Alhajjaj, S. and Kelley, S. (2003), "Using CobiT to Secure Information Assets," *The Journal of Government Financial Management*, 52 (2): 22-32.

Hunton, J.E., Bryant, S.M. and Bagranoff, N.A. (2004), Core Concepts of Information Technology Auditing, John Wiley, Hoboken, NJ.

Kruse, W.G. and Heiser, J.G. (2002), *Computer Forensics: Incident Response Essentials*. Addison Wesley, Indianapolis, IN.

Lange, M.C.S. (2003), "Sarbanes-Oxley Has Major Impact on Electronic Evidence," *The National Law Journal*, Retrieved May 1, 2006 from http://www.law.com/jsp/article.jsp?id=1039054510969

Logan, D. and Mogull, R. (June 22, 2004), "Sarbanes-Oxley: The Role of Technology," *CIO M*agazine, Retrieved May 1, 2006 from www.cio.com.

Naik, B. (2003), "Learning Styles of Business Students," Proceedings of the 34th Annual Meeting of the Decision Sciences Institute, Washington, D.C, November 22-25, 2003.

Nelson, B., Phillips, A., Enfinger, F. and Steuart, C. (2006), *Guide to Computer Forensics and Investigations*, Thomson Publishing, Boston, MA.

O'Donnell, J. and Moore, J. (2005), "Are Accounting Programs Providing Fundamental IT Knowledge?" The CPA Journal, 75 (5): 64-66.

Posthumusa, S. and Solms, R. (2005), "IT Oversight: An Important Function of Corporate Governance," *Computer Fraud & Security*, 6: 11-17

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

Sommer, P. (2004), "The Future for the Policing of Cybercrime," *Computer Fraud and Security*, (2004) 1: 8-12.

Statement on Auditing Standard 94 (2001), "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit," *American Institute of Certified Public Accountants Auditing Standards Board*.

Statement on Auditing Standard 99 (2002), "Consideration of Fraud in a Financial Statement Audit," *American Institute of Certified Public Accountants Auditing Standards Board*.

Vacca, J.R. (2002), *Computer Forensics: Computer Crime Scene Investigation*, Charles River Media, Inc., Hingham, MA.

Websense (2006) "Security Trends Report, Second Half 2005." View at: http://www.websense.com/global/en/.

Wilding, E. (2003), "Corporate Cybercrime Trends," *Computer Fraud and Security*, (2003) 6: 4-6.

Worthen, B. (May 15, 2003), "Your Risks and Responsibilities," *CIO Magazine*, Retrieved May 10 from www.cio.com.

APPENDIX A: SAMPLE CLASS SURVEY FOR ACCOUNTING STUDENT IT AND FORENSICS KNOWLEDGE

Instructions: The purpose of this survey is to assess the average level of knowledge of students in this class in order to better plan lecture materials. Answer the following questions by circling the appropriate answer. Do not be concerned if your answers indicate a low level of current knowledge.

1	Have you had a course in fraud examination?	Yes No
2	Have you had a course in forensics accounting?	Yes No
3	Have you had a course in computer forensics?	Yes No
4	Are you familiar with the COBIT control model?	Yes No
5	Are you familiar with legal issues for IT auditors?	Yes No

Circle the answer that best indicates your level of knowledge.

6	How good is your IT auditing knowledge?	very low	low	average	high	very high
7	How good is your knowledge of cyber crime?	very low	low	average	high	very high
8	How good is your knowledge of computer hardware?	very low	low	average	high	very high
9	How good is your knowledge of computer software?	very low	low	average	high	very high
10	How good is your understanding of relational databases?	very low	low	average	high	very high
11	How good is your understanding of IT disaster planning?	very low	low	average	high	very high
12	How good is your understanding of computer assisted audit tools and/or generalized audit software?	very low	low	average	high	very high

APPENDIX B: A SAMPLE TEACHING PLAN FOR IT INVESTIGATIVE TECHNIQUES COURSE

Week	Topics
1	Review of syllabus The expanded role of internal and external auditors Overview of: COSO, COBIT, SAS 99 & Sarbanes Oxley Group topic paper assignments
2	The information technology function Operating systems, networks, servers and firewalls Attacks on networks Disaster recovery planning
3	Review of database architecture (hierarchical and relational) Disk structures: FAT 32 and NTFS Hidden files and slack space
4	Secret and public key encryption Digital signatures and certificate authorities Demonstration of encryption and hashing Privacy issues and WebTrust
5	Management and corporate fraud and the cyber criminal Internal controls in an IT environment Problems with separation of duties and compensating controls
6	Investigative fraud techniques Signs of embezzlement, collusion, ghost vendors, fictitious revenues The IT audit Responsibilities of internal and external auditors
7	Financial analysis and important ratios for investigation Imaging data without corrupting the chain of custody
8	Mid-term Exam Presentation of group topic papers
9	CAATs Auditing with and through the computer Check digits
10	Log files and analyzers Freezing the digital crime scene and data handling Protecting the chain of custody Confronting the suspect
11	Using ACL ACL Case 1: Look for Duplicates & Gaps, Statistics
12	ACL Case 2: Benford Analysis, Count, Classify
13	ACL Case 3: Examine Sequence, Aging
14	Legal aspects of reporting fraud and cyber crimes Corporate protocols for fast response
15	E-mail protocols, e-mail logs and tracing e-mails Corporate policy on passwords, remote access, whistleblowers
16	Final Exam