Paper Session III: Research Brief: A Curriculum for Teaching Information Technology Investigative Techniques for Auditors

Grover S. Kearns
University of South Florida St. Petersburg

Elizabeth V. Mulig
University of South Florida St. Petersburg

Follow this and additional works at: https://commons.erau.edu/adfsl

Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL

*** RESEARCH BRIEF ***

A Curriculum for Teaching Information Technology Investigative Techniques for Auditors

Grover S. Kearns
Assistant Professor of Accountancy and Information Systems
College of Business
University of South Florida St. Petersburg
St. Petersburg, Florida 33701-5016 USA
727-873-4085
727-873-4192 (fax)
gkearns@stpt.usf.edu

Elizabeth V. Mulig
Assistant Professor of Accountancy
College of Business
University of South Florida St. Petersburg
St. Petersburg, Florida 33701-5016 USA
727-873-4154

Research Brief

Recent prosecutions of highly publicized white-collar crimes combined with public outrage have resulted in heightened regulation and greater emphasis on systems of internal control. Because both white-collar and cybercrimes are usually perpetrated through computers, 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. Furthermore, many students are not instructed in the use of computer assisted auditing tools and techniques – applications that might uncover fraudulent activity. Only a limited number of university-level accounting classes provide instruction in IT investigative techniques.

The first 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. Often it is the auditor that first recognizes that 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.

Business reliance on IT is well documented (Hunton et al. 2004; Posthumusa et al. 2005) and is reflected in auditing statements such as SAS 99 and control documents such as COBIT and the IT control objectives for Sarbanes-Oxley.

Accounting programs may be outdated, not reflecting major changes in the business environment. As a result, students are not equipped with the skills they will actually need in practice (Gabbin 2002). A survey of accounting students in Britain found that they 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).

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.

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.

References will be provided upon request by the contact author.