Improvements in Audit Risks Related to Information Technology Frauds

Saeed Askary, Abu Dhabi University, UAE
David Goodwin, University of Wollongong in Dubai, UAE
Roman Lanis, University of Technology, Sydney, Australia

ABSTRACT

In this paper, the authors examine how different types of fraud in most Information Technology (IT) environments affect an audit risk model from 2001 through 2008. Variations in IT fraud are questionable for determining the audit risks that affect audit quality and report. The data sources in this study came from the Computer Crime and Security Survey report (CSI) 2008. By relating different IT fraud to audit risk components through trend analysis in IT fraud improvements from 2001 to 2008, the authors measured declined percentages for control risks, inherent risks, and detection risks. They found that an improvement in control risks has been achieved up to 52.80%, 43% for detection risks, and 14% for inherent risks. An overall improvement in audit risk is 47.5%, which is a considerable development in audit quality. The study shows that progress in detecting IT fraud positively reduced audit risks and has significantly increased the audit quality since 2001.

Keywords: Audit Risk, Computer Crime and Security, Control Risks, Detection Risk, Information Technology (IT) Fraud, Inherent Risks

INTRODUCTION

Enron, the USA’s largest energy company, collapsed as the largest corporate failure in US history in 2001. The role of Arthur Andersen in this event dented the public trust on the accounting and auditing profession and financial reporting practices. In response to the collapses, enormous efforts have concentrated on rebuilding investors and the public trusts.

The Sarbanes-Oxley (SOX) Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act, was a US federal law in response to the corporate and accounting scandals. The Act establishes a new quasi-public agency, the Public Company Accounting Oversight Board (PCAOB) which is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies. The Act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure. The legislation is wide-ranging and establishes

DOI: 10.4018/jeis.2012040104
new or enhanced standards for all U.S. public company boards, management, and public accounting firms. The ultimate purpose of the legislation would be ideally to produce the most reliable financial information for different user of that information. If auditors are supposed to achieve this goal, they should manage and reduce the audit risk. The lower audit risks inevitably increase audit report quality.

Recent corporate collapses and the new guidelines and legislation of Sarbanes-Oxley Act emphasize the importance of audit risks. Risk assessment in an audit environment is one of essential tasks of every external auditor. Adams et al. (2005) argue that “… clients with greater risk of fraud are less likely to engage prospective auditors in competitive bidding, consistent with the theory that these companies seek to limit access to information that might reveal their high-risk status” (p. 417). Audit risks have three components in a classic view including inherent risk, control risk and detection risk. Auditors of the financial statements are practically exposed to minimize audit risk at the actual lowest possible level. If an auditor fails to do this, then not only nature, timing and extent of other substantive procedures will be affected but also it sometimes causes to issue a wrong audit report that indeed bears auditors with heavy legal penalties. As a result, the risk of producing wrong audit reports is high when audit risk is high. According to Chemuturi (2008, p. 6): “Evaluating fraud risk factors is probably the most difficult part of assessing overall audit risk, and owes its complexity to the fact that human behavior cannot be predicted with certainty. A recent study by the Association of Certified Fraud Examiners estimated that US organizations lose approximately 5% of annual revenue to fraud.”

The reliability of information is significantly affected by the design of the computerized internal controls systems (Kearns & Baker, 2011). As IT systems prevail all over today business entities’ systems of almost all-type sizes and integrated with the internal control systems in many ways (Fukukawa et al., 2006), therefore auditors should consider their due care and skill for understanding the internal control to perform control tests during audit engagements (ISA 315). IT systems are complex by its natures and detecting any types of risks related to information systems, frauds, crimes and IT attacks causes many financial and non-financial damages to their clients. As a result, IT frauds are complex in nature and auditor expose to higher risks to those IT frauds where those frauds eventually will affect the reliability of financial statement of auditors’ client.

Despite how to detect IT frauds, we evaluate how did IT frauds detections audit risks’ components in this study. Although there are recently plenty of research on audit risks and fraud, but effect on a lack of investigation exists on how the IT frauds impact on audit risk model. This research enhances to the previous literature by establishing a contractual framework to analysis IT frauds in audit risk model. Then, we measure arithmetically the frauds in term of either increase or decrease in audit risk components and model.

This investigation is innovative by looking at the CSI survey to understand the trend in different IT frauds and integrated them with inherent, detection and control risk to measure the level of improvements in whole audit risk model. This paper relates theoretical and practical issues of audit risks with different IT frauds. The rest of the paper is organized in five sections. First, a discussion is provided about the audit risk and defines the auditors’ responsibilities to understand and have enough knowledge and skills of their client IT environment and IS. Then, IS risks are identified following up the methodology and results of the study. This is followed by the study’s conclusions and limitations.

RESEARCH BACKGROUND

Research on audit risk and fraud in IT environments has been a subject for many researches recently (e.g., Johnstone, 2008; Malone, 2005; Munter, 2002; Patterson & Noel, 2003; Verschoor, 2010). According to Ernest and Young
Enterprise Information System Security: A Life-Cycle Approach
www.igi-global.com/chapter/enterprise-information-system-security/48540?camid=4v1a

Measuring the Impact of an ERP Project at SMEs: A Framework and Empirical Investigation
Maria Argyropoulou, George Ioannou, Dimitrios N. Koufopoulos and Jaideep Motwani (2010). Enterprise Information Systems for Business Integration in SMEs: Technological, Organizational, and Social Dimensions (pp. 1-14).
www.igi-global.com/chapter/measuring-impact-erp-project-smes/38189?camid=4v1a