International Journal of Accounting Information Systems 18 (2015) 26–45

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

An information security control assessment methodology for organizations' financial information

Angel R. Otero *

Florida Institute of Technology, Nathan M. Bisk College of Business, 150 W. University Blvd., Melbourne, FL 32901, United States

ARTICLE INFO

Article history:
Received 26 July 2014
Received in revised form 26 May 2015
Accepted 12 June 2015
Available online 3 July 2015

Keywords:
Assessment
Design science research
Evaluation
Fuzzy logic
Fuzzy set theory
Information security controls

ABSTRACT

In an era where dependence of information systems is significantly high, the threat of incidents related to information security that could jeopardize financial information held by organizations is serious. Alarming facts within the literature point to inadequacies in information security practices, particularly the evaluation of information security controls in organizations. Research efforts have resulted in various methodologies developed to deal with the information security controls assessment problem. A closer look at these traditional methodologies highlights various weaknesses that prevent an effective information security controls assessment in organizations. This paper develops a methodology that addresses such weaknesses when evaluating information security controls in organizations' financial systems. The methodology uses the fuzzy set theory which allows for a more accurate assessment of imprecise criteria than traditional methodologies. It is argued that using the fuzzy set theory to evaluate information security controls in organizations addresses existing weaknesses identified in the literature and leads to a more precise assessment. This, in turn, results in a more effective selection of information security controls and enhanced information security in organizations. The main contribution of this research is the development of a fuzzy set theory-based assessment methodology that provides for a thorough evaluation of information security controls in organizations. Overall, the methodology presented herein proved to be a feasible technique for evaluating information security controls in organizations' financial systems.

1. Introduction

Throughout the years, organizations have experienced numerous losses which have had a direct impact on their information. Fraud and economic crimes are certainly examples. The Federal Bureau of Investigation (FBI) reported that, in 2011 alone, there were 726 pending corporate fraud cases in the United States (U.S.) involving accounting schemes designed to deceive investors, auditors, and analysts regarding the true financial condition of a corporation. Economic crime (or white-collar crime) also continues to remain in the forefront of corporate concern, posing threats to businesses. The U.S. Supplement 2014 Global Economic Crime Survey, performed by PricewaterhouseCoopers LLP, featured the views of more than 5000 participants from over 100 countries on the prevalence and direction of economic crime since 2011. The survey revealed that 54% of U.S. participants reported their companies experienced fraud in excess of $100,000 with 8% reporting fraud in excess of $5 million. Additionally, the 2009 CSI/FBI Computer Crime and Security Survey (conducted on 443 information security and information technology (IT) professionals in the U.S.) found that average information security losses in organizations, leading to computer security breaches, reached approximately $234,300 per respondent. Moreover, in a study performed by Bedard et al. (2008), about 21% of all deficiencies detected in selected

* Tel.: +1 321 674 8782.
E-mail address: aotero@fit.edu.

http://dx.doi.org/10.1016/j.accinf.2015.06.001
1467-0895/

audited organizations were related to information security. Particularly, Bedard et al.'s (2008) study noted that there were no adequate information security controls (ISCs) in place within the organizations examined, and the ones in place were not operating effectively.

Another fact in today's organizational culture is that most information security challenges are being addressed through the use of security tools and technologies, such as encryption, firewalls, access management, etc. (Singh et al., 2013). Although tools and technologies are an integral part of organizations' information security plans, it is argued that they alone are not sufficient to address information security problems (Herath and Rao, 2009). To improve overall information security, organizations must evaluate (and thus implement) appropriate ISCs that satisfy their specific security requirements (Barnard and Von Solms, 2000; Karyda et al., 2004; Da Veiga and Eloff, 2007). However, due to a variety of organizational-specific constraints (e.g., costs, availability of resources), organizations do not have the luxury of selecting and implementing all required ISCs.

Adequate evaluation of ISCs is crucial to organizations in maintaining sound information security as well as in protecting their financial information assets. Nevertheless, the literature points out several issues, gaps, and/or weaknesses within traditional ISC assessment methodologies that prevent an effective assessment of ISCs in organizations. The weaknesses identified in the literature not only affect the ISC selection process, but also impact the overall protection of the information's confidentiality, integrity, and availability (Saint-Germain, 2005). In other words, the lack of adequate information security over valuable, sensitive, or critical financial information may allow for: (1) fraud, manipulation, and/or misuse of data; (2) security-related deficiencies and findings; (3) bogus trades to inflate profits or hide losses; (4) false accounting journal entries; (5) computer security breaches; and (6) false transactions to evade regulators, among others.

In order to increase the effectiveness of the evaluation and selection process for ISCs in organizations, effective and efficient assessment methods need to be developed. Development of such assessment methodology constitutes a significant contribution to the information security literature. The aim of this paper or research problem is, therefore, to develop a new ISC assessment methodology that adequately addresses the existing weaknesses identified in traditional ISC assessment methodologies. The new methodology is expected to deliver rich information about the research problem, as well as enhance current evaluation methods, ultimately improving information security in the organization.

The fuzzy set theory (FST) allows for a more adequate representation of imprecise parameters than existing methodologies. An evaluation of ISCs using FST could therefore lead to a thorough, more detailed assessment by providing precise values, ultimately improving information security in the organization. Moreover, except for studies performed by Zlateva et al. (2011) and Schryen (2010), which used fuzzy logic to estimate real estate investment risks, and to model security investment decisions, respectively, to the best of the author's knowledge, there have been no other research studies within the literature that have specifically evaluated and prioritized ISCs in organizations using FST (Ejnioui et al., 2012; Otero et al., 2012a,2012b).

2. Literature review and research questions

Following are descriptions of the approaches and methodologies used in organizations regarding ISC evaluations, including several weaknesses identified within them. The emergence of these methodologies in the U.S. has mainly been the result of various laws and regulations on internal controls (particularly related to financial reporting), as established by Sections 404 and 302 of the Sarbanes-Oxley Act of 2002, Public Company Accounting Oversight Board (PCAOB) Auditing Standards, the Federal Deposit Insurance Corporation Improvement Act (FDICIA), and the Securities and Exchange Commission (SEC), among others.

2.1. Risk analysis and management

Risk analysis and management (RAM) is just one example. RAM consists of performing business analyses as well as risk assessments, resulting in the identification of information security risks (i.e., requirements) (Barnard and Von Solms, 2000). RAM would then list the information security requirements as well as the proposed ISCs to be implemented to mitigate the risks resulting from the analyses and assessments performed. RAM, however, has been described as a subjective, bottom-up approach (van der Haar and von Solms, 2003), not necessarily taking into account the organizations' specific constraints. According to Dhillon and Torkzadeh (2006), RAM is not identified as the best or fundamental mean to ensure information security. Dhillon and Torkzadeh (2006) state that organizations, when performing RAM, establish controls that are either unnecessary or relate to trivial issues. Furthermore, exclusive reliance on RAM has often been criticized since it has proven to be more problematic for maximizing information security rather than beneficial. Beginning here, methodologies reviewed such as RAM are referred to as *M* plus the number of the methodology reviewed. For instance, RAM will be referred to as M1.

2.2. Baseline manuals or best practice frameworks, ad-hoc approaches

Baseline manuals or best practice frameworks (M2) are widely used by organizations to introduce ISCs in organizations (Barnard and Von Solms, 2000; Saint-Germain, 2005). Some best practices include: Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL), and the National Institute of Standards and Technology (NIST). Da Veiga and Eloff (2007) also mention other best practice frameworks which have assisted the identification and selection of ISCs, such as, ISO/IEC 177995, ISO/IEC 27001, ISO/IEC 27002, PROTECT, Capability Maturity Model (CMM), and Information Security Architecture (ISA). The process of selecting the most effective ISC from baseline manuals or best practice frameworks is a challenging one. van der Haar and von Solms (2003) state that baseline manuals or best practice frameworks leave the identification of ISC to the