Evaluation of System Change Controls Using Fuzzy Set Theory

Angel R. Otero
Florida Institute of Technology

ABSTRACT

Attacks on information are an ever-increasing threat to every industry. For years, organizations have been a primary target for attacks by cybercriminals largely because of the significant value of the confidential and sensitive information they host. To protect the information, organizations require general information technology controls to be well designed, implemented, and to operate effectively and in compliance with laws and regulations. General information technology controls related to change management (or system change controls), for example, are critical in ensuring the integrity, completeness, and reliability of financial information. Alarming facts within the literature evidence inadequate change management practices and prompt for the identification of additional methods to assist organizations in protecting their sensitive and critical information. The literature shows traditional change management assessment methodologies that do not promote an effective evaluation, prioritization, and, therefore, implementation of system change controls in organizations. This research prompts for the development of a decision support methodology that can accurately prioritize system change controls in organizations. The methodology uses fuzzy set theory to allow for a more accurate assessment of imprecise parameters than traditional methodologies. It is argued that evaluating system change controls using fuzzy set theory leads to a more detailed and precise assessment and, therefore, supports an effective selection of system change controls in organizations.

Keywords: General IT controls, change management, system change controls, fuzzy set theory, assessment, evaluation

1. INTRODUCTION

Attacks on information are an ever-increasing threat to every industry. For years, organizations have been a primary target for attacks by cybercriminals largely because of the significant value of the confidential and sensitive information they host. To protect the information, organizations require internal controls to be well designed, implemented, and to operate effectively and in compliance with laws and regulations (Lavion, 2018). Internal controls refer to procedures and activities implemented by management to mitigate the risks that could prevent a company from achieving its business objectives (Deloitte, 2018; GTAG 8, 2009).

Business objectives, such as, reliability of the entity's financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations are common objectives constantly threatened in an organization (Otero, 2018; Otero, Ejnioui, Otero, & Tejay, 2011). Internal controls should be in place and monitored to ensure the objectives above are met and potential security concerns are reduced or eliminated (Otero, Tejay, Otero, & Ruiz, 2012).

Internal controls related to IT or General IT Controls (GITC) aid in the protection of business operations by securing the integrity, completeness, and reliability of financial information, as well as of any other system functionality underlying business processes (Deloitte, 2018; Otero, 2015). GITC refer to policies and procedures put in place to support the effective functioning of applications, the integrity of reports generated from those applications, and the security of data housed within the applications.

Ineffective GITC (deficiencies) may prevent organizations from generating complete and accurate financial reports (Masli, Richardson, Watson, & Zmud, 2016; Krishnan & Visvanathan, 2007). Deficiencies in GITC, if not timely identified and addressed, may also impact the overall functioning of internal controls, result in delayed financial closing processes, increase audit costs, and impact internal decisions and/or public disclosure, ultimately affecting the reputation and brand of the organization.

GITC commonly include controls over (1) data center and network operations (also referred to as information systems operations); (2) information or access security; and (3) change management. Change management includes controls around the areas of system software acquisition; change and maintenance; program change; and application system acquisition, development and maintenance. Change management are also referred to as system change controls (SCC).

SCC are critical in ensuring the security, integrity, completeness, and reliability of financial information (Keef, 2019; GTAG 2, 2012; Ejnioui, Otero, Tejay, Otero, & Qureshi, 2012). SCC include controls related to each relevant technology elements within the organization's IT environment: application system, database, operating system, and network. Examples of SCC include review, monitoring, and/or approval of system change requests; as well as upgrades to applications, databases, and network infrastructure. Given the significance and rapid integration of IT systems with business processes, SCC must be in place to maintain the completeness and accuracy of information, as well as the reliability of business processes within the organization.

1.1 Current IT Environment

Throughout the years, organizations have experienced numerous system losses that have had a direct impact on their most valuable asset, information. Schwartz (1990) stated that system losses related to confidential and sensitive financial information will continue to happen and their effect will be devastated to organizations. Examples of such information

losses result from inaccurate calculations, unreliable system processing, incomplete recording of data, lost data, cutoff errors, and other misstatements of the accounting records (ISACA, 2011; Otero, 2015).

According to the Federal Bureau of Investigation's (FBI) (2019), white-collar crime or corporate fraud continues to be one of the FBI's highest criminal priorities. Corporate fraud results in significant financial losses to companies and investors, and continue causing immeasurable damage to the U.S. economy and investor confidence. FBI (2019) states that the majority of corporate fraud cases pursued mostly involve accounting schemes, such as: false accounting entries and/or misrepresentations of financial condition; fraudulent trades designed to inflate profits or hide losses; and/or illicit transactions designed to evade regulatory oversight. The above schemes are designed to deceive investors, auditors, and analysts about the true financial condition of a corporation or business entity. Through the manipulation of financial data, share price, or other valuation measurements, financial performance of a corporation may remain artificially inflated based on fictitious performance indicators provided to the investing public. To add to the above, in a Global Economic Crime Survey performed by PricewaterhouseCoopers LLP (2014), the views of more than 5,000 participants from over 100 countries were featured on the prevalence and direction of economic crime since 2011. The survey revealed that 54% of U.S. participants reported their companies experienced fraud or inconsistencies with their financial systems in excess of $100,000 with 8% reporting fraud in excess of $5 million. Moreover, the use of web applications (which has grown exponentially in the recent years) has brought in security risks and vulnerabilities around financial information creating significant exposure for many organizations (ISACA, 2011; Thomé, Shar, Bianculli, & Briand, 2018). The alarming facts and figures above all point to an inadequacy in today's IT environment and serve as motivation for finding new ways to help organizations improve their capabilities for securing, managing, and controlling valuable information.

Currently, most of the challenges related to information security and change management practices are addressed through the use of tools and technologies (Singh, Picot, Kranz, Gupta, & Ojha, 2013; Volonino & Robinson, 2004; Vaast, 2007). However, it is argued that these tools and technologies alone are not sufficient to address the information security and change management problems just presented (Keef, 2019; Herath & Rao, 2009). To improve overall change management practices, for example, organizations must evaluate (and thus implement) appropriate SCC that satisfy their specific security requirements (Barnard & Von Solms, 2000; Da Veiga & Eloff, 2007; Karyda, Kiountouzis, & Kokolakis, 2004). However, due to a variety of organizational-specific constraints (e.g., cost, scheduling, resources availability, etc.), organizations do not have the luxury of selecting and implementing all required SCC. Therefore, the selection and implementation of SCC within organizations' business constraints become a non-trivial task.

The concerning facts and figures above evidence the lack of adequate change management practices and clearly suggest the identification of additional methods to assist organizations in protecting their sensitive and critical information. One of those methods is through the effective implementation of SCC to maintain a well-designed and controlled information system environment. Nevertheless, change management is at its best in organizations when only the most appropriate SCC are implemented.

The literature shows traditional change management evaluation methodologies that do not promote an effective assessment, prioritization, and, therefore, implementation of SCC in organizations. For instance, the selection of SCC in organizations based on traditional methods has been determined through using crisp or dichotomous values (i.e., yes or no type answers). This means that organizations perform their selection based on whether the SCC is either relevant or not. The problem here is that imprecision, which considers the degree of relevance

or significance for each SCC, is not being considered. Evaluation of SCC must address and measure how relevant SCC are (i.e., calculating degrees of relevance) prior to their selection. The aforementioned illustrates a major problem that can potentially impact the overall security over organizations' valuable, sensitive, or critical information.

This research prompts for the development of a decision support methodology that can accurately prioritize SCC in organizations. A methodology that considers imprecise parameters (in the form of organizations' criteria) when evaluating SCC, and rank such parameters using real numbers represents a major step for organizations, as well as a significant contribution to the literature. The remainder of this research paper is organized as follows. Section 2 provides a summary of the literature reviewed on SCC evaluation and selection. Section 3 explains the theory to be used in the development of the proposed methodology. Section 4 describes the proposed solution approach. Section 5 discusses contributions, limitations, and opportunities for future research. Section 6 provides a summarized conclusion.

2. LITERATURE REVIEW

Various reasons have been put forth for explaining the lack of effectiveness in the evaluation, selection, and implementation process of controls. Wood (2000) argues that the implementation of controls in organizations may constitute a barrier to progress. For instance, participants from the ICIS 1993 conference panel indicated that the implementation of controls may slow down production thereby turning the employees' work ineffective (Loch, Conger, & Oz, 1998). Employees may view controls as interrupting their day-to-day tasks (Post & Kagan, 2007) and may, therefore, tend to ignore implementing them in order to be effective and efficient with their daily job tasks.

According to Saint-Germain (2005), organizations are required to identify and implement appropriate controls to ensure adequate information security. Baskerville and Siponen (2002) place emphasis on the fact that "different organizations have different security needs, and thus different security requirements and objectives" (p. 344). Whitman, Towsend, and Aalberts (2001) also stress that there is no single information security solution that can fit all organizations. As a result, controls must be carefully selected to fit the specific needs of the organization. Identification and implementation of the most effective controls is a major step towards providing an adequate IT environment in organizations (Barnard & Von Solms, 2000).

2.1 Previous Approaches in the Selection and Evaluation of SCC in Organizations

Based on Barnard and Von Solms (2000), the process of identifying (and selecting) the most effective SCC in organizations has been a challenge in the past, and plenty of attempts have been made to come up with the most effective way possible. Risk analysis and management (RAM) is just one example. RAM has been recognized in the literature as an effective approach to identify SCC (Barnard & Von Solms, 2000). RAM consists of performing business analyses as well as risk assessments, resulting in the identification of information security requirements (Barnard & Von Solms, 2000). RAM would then list the information security requirements as well as the proposed SCC 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 & Von Solms, 2003), not taking into account organizations' specific constraints. For example, through performing RAM, organizations may identify 25 change management-related risks. Nonetheless, management may not be able to select and implement all necessary SCC to

address the previously identified 25 risks due to costs and scheduling constraints. Moreover, there may not be enough resources within the organization to implement these SCC. In this case, management should lists all those risks identified and determine how critical each individual risk is to the organization, while considering costs versus benefits analyses. Management must therefore explore new ways to determine and measure the relevancy of these SCC considering the constraints just presented.

Baseline manuals or best practice frameworks is another approach widely used by organizations to introduce minimum controls in organizations (Barnard & Von Solms, 2000). Saint-Germain (2005) states that best practice frameworks assist organizations in identifying appropriate SCC. Some best practices include: Control Objectives for Information and related Technology (COBIT), ITIL Change Control, the National Institute of Standards and Technology (NIST), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). Da Veiga and Eloff (2007) mentioned other best practice frameworks that have also assisted in the identification and selection of SCC, such as, International Standardization Organization (ISO) / International Electrotechnical Commission (IEC) 27001 and 27002 and the Capability Maturity Model.

Selecting effective SCC from best practice frameworks can be challenging (Van der Haar & Von Solms, 2003). Van der Haar and Von Solms (2003) state that best practice frameworks leave the choosing of controls to the user, while offering little guidance in terms of determining the best controls to provide adequate protection for the particular business situation. Additionally, frameworks do not take into consideration organization specific constraints, such as, costs of implementation, scheduling, and resource constraints. Other less formal methods like ad hoc or random approaches could lead to the inclusion of unnecessary controls and/or exclusion of required/necessary controls (Barnard & Von Solms, 2000). Identifying and selecting SCC based on the above may result in organizations not being able to protect the overall confidentiality, integrity, and availability of their information (Saint-Germain, 2005). In order to increase the effectiveness of the selection and prioritization process for SCC, new methods need to be developed that save time while considering major factors (e.g., constraints, restrictions, etc.) that undoubtedly affect the selection of such controls.

In another study, Gerber and von Solms (2008) created a Legal Requirements Determination Model (LRDM) for defining legal requirements, which in turn, indicated relevant controls to be selected from the list provided in the ISO/IEC 27002 best practice framework to satisfy the identified legal requirements. Specifically, the authors: (1) developed a structured model to assist in establishing information security requirements from a legal perspective; (2) provided an interpretation of the legal source associated with information security requirements; and (3) proposed potential controls from the ISO/IEC 27002 best practice framework to address the already identified legal information security requirements. Legal information security requirements were determined by devising and utilizing a legal compliance questionnaire in combination with a legal matrix that included mappings of legal aspects within each of the proposed legal categories to all related ISO/IEC 27002 controls. Following determination of the legal requirements, a list of relevant controls from the ISO/IEC 27002 framework, including SCC, was produced to satisfy the previously identified legal requirements.

Nonetheless, as evidenced earlier, the selection of controls from baseline manuals or best practice frameworks, as it is the case with the LRDM using the ISO/IEC 27002 framework, represents a weakness. Baseline manuals or best practice frameworks offer little guidance in terms of determining the best controls to provide adequate security for the particular business situation (van der Haar & von Solms, 2003). Furthermore, baseline

manuals or frameworks do not necessarily take into consideration organization specific constraints, such as costs, scheduling, and resource constraints.

The literature just presented evidences limitations in existing SCC assessment methodologies. A methodology based on fuzzy set theory (FST) allows for a more accurate assessment of imprecise parameters than traditional methodologies (Zimmermann, 2010). That is, evaluation of SCC using FST will result in a thorough assessment (Zimmermann, 2010), supporting a more effective SCC evaluation and prioritization. Furthermore, based on the literature reviewed, there has not been other research study within the academic literature that specifically evaluated and prioritized SCC in organizations using FST. The proposed methodology adds practical value, as it will help management to accurately identify which SCC need to be selected and implemented in order to ensure adequate safeguarding of the information.

3. THEORETICAL BASIS

3.1 Fuzzy Logic System

Based on Zimmermann (2010), the majority of traditional tools for formal modeling, reasoning, and computing are crisp, deterministic, and/or precise in character. Crisp refers to dichotomous, meaning yes or no type answers, rather than a more-or-less type. When dealing with traditional dual logic, for example, statements can be either true or false, nothing else. This implies that the decision of whether an element belongs to a set is unequivocal and has no ambiguities. That is, parameters within a model are known and there are no doubts about their values or their occurrence. Reference to Zimmermann (2010) indicates that these types of (logic) assumptions do not correctly describe reality; and that the "complete description of a real system would often require far more detailed data than a human being could ever recognize simultaneously, process, and understand" (p. 317).

According to Klir and Yuan (1995), logic refers to the study of methods for reasoning. Logic can be classical or fuzzy. Classical logic relies on the assumption that propositions are either true or false. In fuzzy logic, however, propositions can be true to some degree, allowing for logical reasoning with partially true imprecise statements (Das, 2009). That is, in fuzzy logic, the truth values are no longer restricted to the two values 'true' and 'false', but expressed by the linguistic variables 'true' and 'false' (Zimmermann, 2010).

3.2 Fuzzy Set Theory

FST refers to an uncertainty theory useful in the absence of probabilities, as well as in the presence of subjective assessments (Schryen, 2010). The idea of FST is, per Schryen (2010), "the extension of the (crisp) membership concept in traditional set theory by providing for a degree with which an element belongs to a set" (p. 8). Such a degree is specified by a membership function. The degree of truthfulness of propositions –grounded on FST– also allows parameters to be represented with simple linguistic terms (Zimmermann, 2010). The association of linguistic terms with membership functions forms fuzzy sets.

Klir and Yuan (1995) state that a "fuzzy set can be defined mathematically by assigning to each possible individual in the universe of discourse a value representing its grade of membership in the fuzzy set" (p. 4). Such a grade refers to the degree to which that individual, entity, etc. is similar or compatible with the concept represented by the fuzzy set. That is, those individuals or entities may belong in the fuzzy set, to a greater or a lesser degree, as indicated by a larger or smaller membership grade (Klir & Yuan, 1995). The membership in

a fuzzy set is not a matter of affirmation or denial, right or wrong, but rather a matter of a degree (Zadeh, 1965).

Membership grades or functions map elements from any universal set into real numbers within the range 0 - 1. The resulting number represents the degree of membership of elements to particular fuzzy sets, where values closer to one represent higher degrees of membership. Figure 1 in the Appendix shows an example of a triangular fuzzy set to denote the SCC RELEVANCE by a particular SCC as a function of a rating from one to 10. Here, a rating of five fully belongs to the fuzzy set; therefore, the degree of membership is 1.0. Ratings of four and six have 0.5 degrees of membership to the fuzzy set, while ratings less than three and greater than seven are not part of the fuzzy set.

There are various forms of membership functions provided by FST. Determining appropriate membership functions is essential for making FST practically useful (Klir & Yuan, 1995). The most common membership functions used to represent fuzzy numbers are: triangular, trapezoidal, and linear shapes. Triangular membership functions are usually preferred due to their combination of solid theoretical basis and simplicity (Pedrycz, 1994). Nevertheless, there are situations where more complex functions may be required to represent the degrees of membership of elements in fuzzy sets. Klir and Yuan (1995) discuss direct/indirect methods to form fuzzy sets by gathering and processing responses from experts, or from literature reviews. Next, the Mamdani Max-Min Method reasoning technique to be utilized for the SCC assessment methodology is discussed.

3.3 Fuzzy Reasoning

Fuzzy reasoning refers to the process of developing logical inferences from imprecise premises (Das, 2009). In classical logic, a widely used inference rule is the modus ponens, which states that a conclusion can be inferred given a conditional proposition and a fact. For instance, a classical modus ponens inference using the relationship between the value of a particular SCC, and its level of priority can be expressed as indicated in Table 1 (Appendix). Table 1 (Appendix) shows that if the generated score of SCC_1 is x (Proposition 1), and x implies a ‘low priority’ SCC as defined by the organization (Proposition 2), then it can be inferred that SCC_1 has a ‘low priority’ and, therefore, must not be selected (Conclusion). Notice that this type of inference structure deals with binary-valued propositions. That is, the solution set to describe the priority level of an SCC is {0, 1} when using the classical modus ponens.

The classical modus ponens must be customized (i.e., generalized) in order to be used for fuzzy reasoning purposes. Such generalization is obtained as follows: first, the generalized version considers degrees of membership of elements to fuzzy sets. This means that the solution set to describe the priority level of SCC is expanded from {0, 1} to [0, 1]. Second, propositions showing completely true implications via the ‘=>’ symbol are replaced with fuzzy rules. Fuzzy rules are conditional and unqualified propositions implying fuzzy relationships between an antecedent and a consequence (Klir & Yuan, 1995). This relationship, also known as a fuzzy implication, is not explicit but rather embedded within the proposition and determined for all values of antecedents and consequences (Demicco & Klir, 2004). The third way to generalize the classical modus ponens is to use the compositional rule of inference, which provides for a fuzzy conclusion given both, a fuzzy rule and a fuzzy fact. The generalized modus ponens inference rule, indicated in Table 2 (Appendix) has been the foundation for various fuzzy reasoning methods presented in the literature (Mizumoto & Zimmermann, 1982; Otero & Otero, 2011).

The inference approach or fuzzy reasoning technique used for this research is the Mamdani Max-Min method, which employs the generalized modus ponens process for each

fuzzy rule. This Mamdani Max-Min method follows the multi-conditional reasoning structure illustrated in Table 3 (Appendix).

Based on the Mamdani Max-Min method, the fuzzy implication (required by the compositional rule of inference) equals the truth value of the antecedent. In other words, the fuzzy implication for singleton fuzzy rules equals the degree of membership of the only statement in the antecedent (Otero & Otero, 2011), and this is indicated in Figure 2A (Appendix). For nonsingleton fuzzy rules, the fuzzy implication is computed as the intersection of the statements in the antecedent via the minimum logical operation (indicated in the Appendix, Figure 2B). An antecedent with a truth value greater than zero automatically implies that its consequence also has a truth value greater than zero. In fuzzy reasoning terms, a true antecedent causes a rule to fire. The fired rules are then combined into a new fuzzy set which will be used to make final inferences (indicated in the Appendix, Figure 2C).

3.4 Defuzzification

Defuzzification converts conclusions from fuzzy sets into a real number, or a single crisp value (Yager, 1996). Available defuzzification methods include the center of gravity approach, which uses integrals to calculate the area of a combination of fuzzy sets, and the common weighted average method. The weighted average method is reliable, less complicated and time consuming, and also used to approximate the center of gravity (Genske & Heinrich, 2009). Figure 2C (Appendix) shows an example of the estimated center of gravity of a fuzzy set composed of two fired fuzzy rules.

4. PROPOSED SOLUTION APPROACH

The proposed solution involves a questionnaire that will be provided to key finance and IT personnel within the organization to determine an initial degree of relevance for SCC. Given that most organizations have Accounting/Finance and IT departments within their organizational structure, it is stated that the target audience does (and will) reflect an accurate representation of the population (Salkind, 2009). The questionnaire will list all SCC that can be potentially implemented in the organization. The list of SCC will be obtained from the ISO/IEC 17795 standard, which is widely used in organizations to select SCC (Da Veiga & Eloff, 2007; Nachin, Tangmanee, & Piromsopa, 2019; ISACA, 2009).

Following collection of questionnaire results and based on the initial degree of relevance of the SCC obtained, analyses will be performed using fuzzy logic/reasoning in order to rank SCC by fusing their respective assessment values into a single, quantified measure using the Mamdani Max-Min fuzzy reasoning technique. This will provide organizations with a measurement of relevance for each SCC based strictly on organizational objectives and goals. The derived relevance measurement can be used as the main metric for evaluating and ultimately selecting SCC.

The solution approach will employ FST to create fuzzy sets of crisp rating levels (very high (VH), high (H), medium (M), low (L), and very low (VL)) for SCC identified from the questionnaires. The rating levels will be defined based on the literature, and supported, validated, and agreed by decision-makers within the organization. Decision-makers will agree on a rating scale from 1 to 5 (i.e., VL, L, M, H, VH), where higher ratings represent a higher criticality and importance of the SCC. This rating scale is commonly used in the industry to describe relevance of controls.

Establishment of linguistic terms (e.g., VH, H, L, etc.) will follow to denote the levels of criticality of SCC based on the crisp ratings assigned. Fuzzy sets will then be created for each linguistic term in order to determine the degrees of membership of crisp evaluation

ratings in each fuzzy set. Lastly, fuzzy reasoning will be used (via the Mamdani Max-Min method) to develop logical inferences from imprecise premises defined by the fuzzy sets, and to thoroughly evaluate, precise, and prioritize each SCC. This detailed evaluation and prioritization will significantly assist management's decision-making process in implementing only the most effective SCC.

5. CONTRIBUTIONS, LIMITATIONS, AND FUTURE RESEARCH

The main contribution of this research to the change management literature is the development of a FST-based assessment methodology that provides a thorough evaluation of SCC in organizations. The proposed methodology addresses the limitations identified in the literature for SCC assessment methodologies, and enhance the overall information security in organizations.

An SCC assessment methodology based on FST provides benefits and advantages over traditional methods, including a strict mathematical methodology that can precisely and rigorously examine vague conceptual phenomena (Zimmermann, 2010). Additionally, FST has been used as a modeling, problem solving, and data mining tool, and has proven superior to existing methods, as well as attractive to enhance classical approaches.

Klir and Yuan (1995) also point the significance of FST when handling uncertainty. FST helps in understanding the phenomenon of reality by performing adequate predictions or retrodictions; learning about controlling the phenomenon; and utilizing such capabilities for various other ends. Furthermore, a FST-based methodology leads to more detailed and thorough assessments, while appropriately modeling human decisions related to SCC evaluation, which are imprecise in nature (Petrovic-Lazarevic, 2001).

A suitable FST-based SCC assessment methodology will account for imprecise parameters and criteria when calculating the relevance of SCC. Such evaluation is also focused on how well SCC address organization objectives, goals, and restrictions. Results from this research should support that a FST-based methodology will, in fact, assist organizations in evaluating and, thus, determining and selecting only the most effective SCC. The methodology presented within this research also lays down the foundation for the development of a fuzzy expert system as a solution to the existing SCC evaluation and ranking problem.

A key advantage of using a FST-based decision support methodology for SCC evaluation is that it provides a natural, effective way of handling problems in which the source of imprecision is the absence of sharply defined criteria. Nevertheless, the solution requires the specification of membership functions of fuzzy sets, definitions of linguistic variables, and fuzzy operators in order to model the attitudes and assumptions of organizations regarding the relevance of SCC. In other words, fuzzy sets must be specified with regard to the objective function, constraints established, as well as terms and membership functions of the linguistic variables. Further empirical work would contribute to identify the aforementioned attitudes and assumptions of decision makers within organizations. Despite the limitation stated above, it is argued that a FST perspective of evaluating SCC is valuable for organizations when dealing with uncertainty and imprecision.

Opportunities for future work may include refinement of the questions included within the questionnaire, or incorporation of additional questions and information that can improve the current investigation. Additionally, future research could examine results from this study as well as from other SCC evaluation methodologies with the purpose of comparing both in order to determine which method is the most effective. A further potential research could be to investigate whether it is reasonable to develop fuzzy rules and baselines of membership functions for SCC in particular environments. In other words, an opportunity for research

could be to interview experts from organizations within similar industries in order to identify fuzzy sets for SCC assessments that can potentially be utilized as guidelines/standards across organizations within similar industries.

6. CONCLUSION

As seen throughout this research, studies continue to support the harmful effects of unsuccessful and/or weak change management practices which result in opportunities for fraud, manipulation of information, and computer breaches, among others. Through a review of the literature, a key limitation identified of current SCC assessment methodologies is that imprecise parameters are being modeled as precise ones. To address this limitation, this a FST-based SCC assessment methodology is proposed. The proposed methodology will assist organizations in accurately evaluating imprecise parameters (i.e., related to the significance of SCC) and, thus, calculating the true relevance of SCC based on how well they address organization objectives, goals, and restrictions. The methodology will also assure organizations that only the best and most appropriate SCC get implemented, while maintaining a well-designed and controlled information system environment.

7. REFERENCES

[1] Barnard, L., & Von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls, *Computers & Security, 19*(2), 185-194.

[2] Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations, *Journal of Logistics Information Management, 15*(1), 337-346.

[3] Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework, *Information Systems Management, 24*(4), 361-372.

[4] Das, P. (2009). Adaptation of fuzzy reasoning and rule generation for customers' choice in retail FMCG business, *Journal of Management Research, 9*(1), 15-26.

[5] Deloitte's Risk Advisory (November 2018). *General IT Controls (GITC) Risk and Impact*. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-general-it-controls-noexp.pdf (accessed May 2019).

[6] Demicco, R. V., & Klir, G. J. (2004). Fuzzy Logic in Geology. Academic Press.

[7] Ejnioui, A., Otero, A. R., Tejay, G., Otero, C. E., & Qureshi, A. (2012). A Multi-Attribute Evaluation of Information Security Controls in Organizations Using Grey Systems Theory. *International Conference on Security and Management*, 1-7.

[8] Federal Bureau of Investigation (FBI). (2019). *White-Collar Crime*. FBI Major Threats & Programs – What We Investigate. www.fbi.gov/investigate/white-collar-crime (accessed April 2019).

[9] Genske, D. D., & Heinrich, K. (2009). A knowledge-based fuzzy expert system to analyze degraded terrain, *Expert Systems with Applications, 36*(1), 2459-2472.

[10] Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects, *Computers & Security, 27*(5), 124-135.

[11] Global Technology Audit Guide (GTAG) 2: *Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition.* The Institute of Internal Auditors. (2012). https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx (accessed April 2019).

[12] Global Technology Audit Guide (GTAG) 8: *Auditing Application Controls*. The Institute of Internal Auditors. (2009). https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx (accessed April 2019).

[13] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness, *Decision Support Systems, 47*(2), 154-165.
[14] ISACA. (2009). COBIT and Application Controls: A Management Guide, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-and-Application-Controls-A-Management-Guide.aspx (accessed May 2019).
[15] ISACA. (2011). Web Application Security: Business and Risk Considerations, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Web-Application-Security-Business-and-Risk-Considerations.aspx (accessed May 2019).
[16] Karyda, M., Kiountouzis, E., & Kokolakis, S. (2004). Information systems security policies: A contextual perspective, *Computer Security, 24*(1), 246-260.
[17] Keef, S. (2019). Why Security Product Investments Are Not Working. ISACA Journal volume 2, 2019. https://www.isaca.org/Journal/archives/2019/Volume-2/Pages/why-security-product-investments-are-not-working.aspx (accessed May 2019).
[18] Klir, G. J., & Yuan, B. (1995). *Fuzzy Sets and Fuzzy Logic: Theory and Applications.* Upper Saddle River, NJ: Prentice Hall PTR.
[19] Krishnan, G. V., & Visvanathan, G. (2007). Reporting Internal Control Deficiencies in the Post-Sarbanes-Oxley Era: The Role of Auditors and Corporate Governance, *International Journal of Auditing, 11*(2), 73-90.
[20] Lavion, D. (2018). *Pulling fraud out of the shadows*. Global Economic Crime and Fraud Survey 2018. PricewaterhouseCoopers LLP, https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html#cta-1 (accessed May 2019).
[21] Loch, K., Conger, S., & Oz, E. (1998). Ownership, privacy and monitoring in the workplace: A debate on technology and ethics, *Journal of Business Ethics, 17*(1), 653-663.
[22] Masli, A., Richardson, V.J., Watson, M.W., & Zmud, R.W. (2016). Senior Executives' IT Management Responsibilities: Serious IT-Related Deficiencies and CEO/CFO Turnover, *MIS Quarterly, 40*(1), 687-708.
[23] Mizumoto, M., & Zimmermann, H. J. (1982). Comparison of fuzzy reasoning methods, *Fuzzy Sets and Systems, 8*(3), 253-283.
[24] Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). *How to Increase Awareness*. ISACA Journal volume 2, 2019. http://www.isacajournal-digital.org/isacajournal/2019_volume_2/MobilePagedArticle.action?articleId=1468061#articleId1468061 (accessed May 2019).
[25] Otero, A. R. (2015). An Information Security Control Assessment Methodology for Organizations' Financial Information, *International Journal of Accounting Information Systems, 18*(1), 26-45.
[26] Otero, A. R. (2018). *Information Technology Control and Audit, 5th Edition*. Boca Raton, FL. CRC Press and Auerbach Publications.
[27] Otero, A. R., Ejnioui, A., Otero, C. E., & Tejay, G. (2011). Evaluation of Information Security Controls in Organizations by Grey Relational Analysis, *International Journal of Dependable and Trustworthy Information Systems, 2*(3), 36-54.
[28] Otero, A. R., Tejay, G., Otero, L. D., & Ruiz, A. (2012). A fuzzy logic-based information security control assessment for organizations. *IEEE Conference on Open Systems*, 1-6. doi:10.1109/ICOS.2012.6417640
[29] Otero, L. D., & Otero, C. E. (2011). A fuzzy expert system architecture for capability assessments in skill-based environments, *Expert Systems with Applications, 39*(1), 654-662.

[30] Pedrycz, W. (1994). Why triangular membership functions?, *Fuzzy Sets and Systems, 64*(1), 21-30.
[31] Petrovic-Lazarevic, S. (2001). Personnel selection fuzzy model, *International Transactions in Operational Research, 8*(1), 89-105.
[32] Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks, *Computers & Security, 26*(3), 229-237.
[33] PricewaterhouseCoopers LLP. (2014). *Economic crime: A threat to business globally*. PwC's 2014 Global Economic Crime Survey, https://www.pwc.at/de/publikationen/global-economic-crime-survey-2014.pdf (accessed May 2019).
[34] Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799, *Information Management Journal, 39*(4), 60-66.
[35] Salkind, N. J. (2009). *Exploring Research (7th ed.)*. Upper Saddle River, NJ: Prentice-Hall, Inc.
[36] Schryen, G. (2010). A fuzzy model for IT security investments. *Proceedings of Sicherheit, Schutz und Zuverlässigkeit*, 289-304.
[37] Schwartz, M. (1990). Computer security: Planning to protect corporate assets, *Journal of Business Strategy, 11*(1), 38-41.
[38] Singh, A.N., Picot, A., Kranz, J., Gupta, M.P., & Ojha, A. (2013). Information security management (ISM) practices: lessons from select cases from India and Germany, *Global Journal of Flexible Systems Management, 14*(4), 225-239.
[39] Thomé, J., Shar, L. K., Bianculli, D., & Briand, L. (2018). Security slicing for auditing common injection vulnerabilities, *Journal of Systems and Software, 137*(1), 766-783.
[40] Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of information systems security in healthcare, *Journal of Strategic Information Systems, 16*(1), 130-152.
[41] Van der Haar, H., & Von Solms, R. (2003). A model for deriving information security controls attribute profiles, *Computers & Security, 22*(3), 233-244.
[42] Volonino, L., & Robinson, S. R. (2004). *Principles and practice of information security, 1st Edition*. Upper Saddle River, NJ: Pearson Prentice Hall, Inc.
[43] Whitman, M. E., Towsend, A. M., & Aalberts, R. J. (2001). *Information systems security and the need for policy*. In G. Dhillon (Eds.), Information Security Management: Global Challenges In The New Millennium (pp 9-18). Hershey, PA: Idea Group Publishing.
[44] Wood, C. (2000). An unappreciated reason why security policies fail, *Computer Fraud and Security, 10*(1), 13-14.
[45] Yager, R. R. (1996). Knowledge-based defuzzification, *Fuzzy Sets Systems, 80*(1), 177-185.
[46] Zadeh, L. (1965). Fuzzy sets, *Information Control, 8*(1), 338-353.
[47] Zimmermann, H. -J. (2010). *Fuzzy Set Theory*. New York, NY: John Wiley & Sons, Inc.

APPENDIX

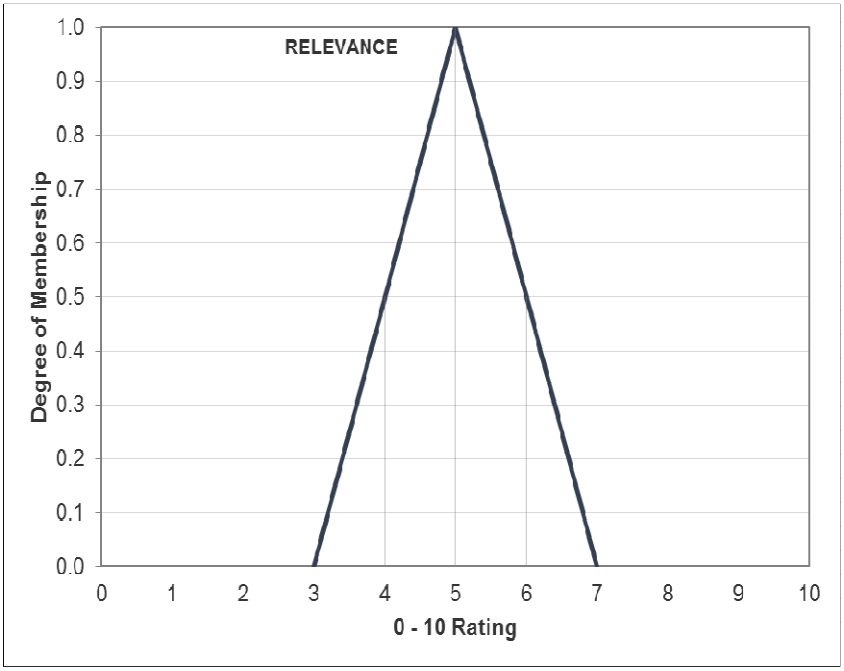

Figure 1: Example of a Triangular Fuzzy Set

Table 1: Classical Modus Ponens

Type of Statement	**Statement**
Proposition 1	Generated score of SCC_1 = x
Proposition 2	'x' $\Rightarrow$ A low priority SCC as specified by the organization
Conclusion	SCC_1 = A low priority SCC

Table 2: Generalized Modus Ponens

Type of Statement	**Statement**
Fuzzy Rule	If x is A, Then y is B
Fact	$\mu_A(x)$
Fuzzy Conclusion	$\mu_B(y)$

Table 3: Multi-conditional Reasoning Structure

Type of Statement	**Statement**

Type of Statement	Statement
Rule 1	If x is A_1, Then y is B_1
Rule 2	If x is A_2, Then y is $B2_2$
…	…
Rule n	If x is A_n, then y is B_n
Fact	$\mu_A(x)$
Conclusion	$\mu_B(y)$

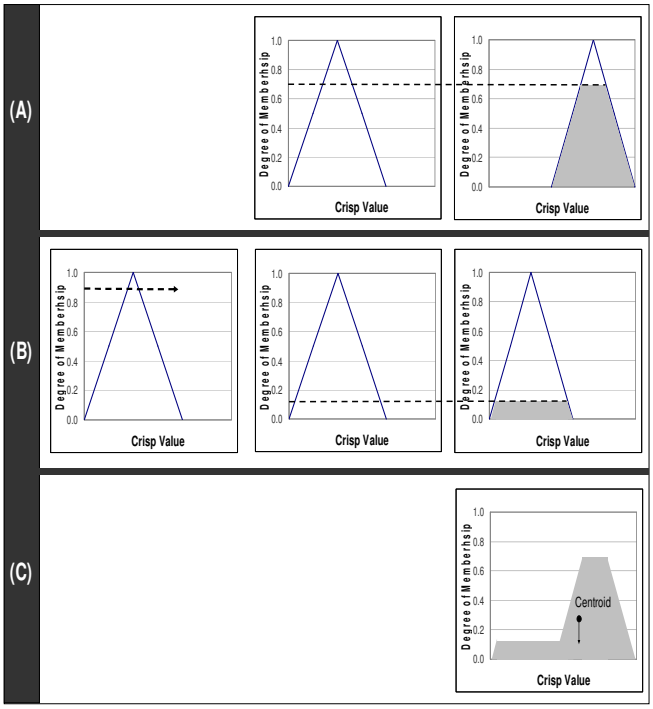

Figure 2: Mamdani Max-Min Inference