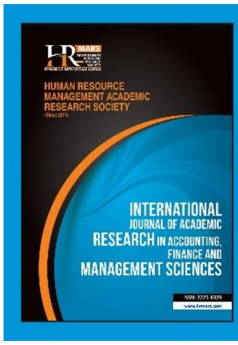


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

HR MARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2225-8329

Enhanced Security over Accounting Data: A Fuzzy-Based Evaluation Model to Aid Organizations in Safeguarding their Accounting Systems

Angel R. Otero

To Link this Article: http://dx.doi.org/10.6007/IJARAFMS/v10-i3/7780 DOI:10.6007/IJARAFMS/v10-i3/7780

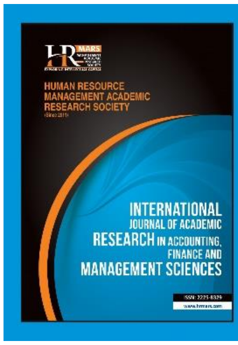
Received: *30 July 2020,* ***Revised:*** *28* August *2020,* ***Accepted:*** *20* September *2020*

Published Online: 16 October 2020

In-Text Citation: (Otero, 2020)
To Cite this Article: Otero, A. R. (2020). Enhanced Security over Accounting Data: A Fuzzy-Based Evaluation Model to Aid Organizations in Safeguarding their Accounting Systems. *International Journal of Academic Research in Accounting, Finance and Management Sciences. 10(3),* 160-175.

Vol. 10, No. 3, 2020, Pg. 160 - 175

http://hrmars.com/index.php/pages/detail/IJARAFMS	**JOURNAL HOMEPAGE**



INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

HR MARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL

www.hrmars.com
ISSN: 2225-8329

Enhanced Security over Accounting Data: A Fuzzy-Based Evaluation Model to Aid Organizations in Safeguarding their Accounting Systems

Angel R. Otero
Assistant Professor, Nathan M. Bisk College of Business, Florida Institute of Technology, Melbourne, FL, U.S.
Email: aotero@fit.edu

Abstract
Attacks on information are an ever-increasing threat to every industry. To protect financial information from accounting applications, organizations require general information technology controls (GITC) to operate effectively and comply with laws and regulations. GITC related to change management or system change controls (SCC) are critical in ensuring the accuracy and completeness of the aforementioned information. Alarmingly, the literature evidences traditional change management assessment methodologies that do not promote effective evaluation of SCC, prompting for the development of additional methods to assist organizations in protecting their financial information. This research proposes the development of a decision-support methodology, using fuzzy set theory, that can better safeguard accounting applications by allowing for a more robust implementation of SCC. It is argued that evaluating SCC using fuzzy set theory leads to a more precise assessment, resulting in a more secure financial environment.

Keywords: General IT Controls, Accounting Applications, System Change Controls, Fuzzy Set Theory, Evaluation

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 information residing on accounting application systems, for example, organizations require internal controls to be well designed, implemented, and to operate effectively and in compliance with laws and regulations (Lavion, 2018; Otero, 2015a). Internal controls refer to procedures and activities implemented by organizations to mitigate the risks that could prevent them from achieving their business objectives (Deloitte, 2018; The Institute of Internal Auditors, 2019).

Business objectives, such as, reliability of the entity's financial reporting, effectiveness and efficiency of operations, as well as 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, Sonnenberg, & Bean, 2019).

Internal controls related to information technology (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, 2015b). 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 (Otero, 2014). GITC commonly comprise controls over (1) data center and network operations; (2) information or access security; and (3) change management. Change management includes controls around the areas of system software acquisition; network architectures; network security; change and maintenance; program change; and application system acquisition, development and maintenance. Change management controls are also referred to as system change controls (SCC).

SCC are critical in ensuring the security, integrity, completeness, and reliability of financial applications and their information (Keef, 2019; The Institute of Internal Auditors, 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 the review and approval of system change requests; as well as procedures to ensure an adequate implementation of upgrades to applications, databases, and network architectures. 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.

Current IT Environment

According to the Federal Bureau of Investigation (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 continues causing immeasurable damage to the U.S. economy and investor confidence. Based on Federal Bureau of Investigation (2019), 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. These schemes are often the result of weakly-implemented controls, particularly SCC (Otero, 2015a; Keef, 2019).

Through 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 Internet and 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 (Thome, Shar, Bianculli, & Briand, 2018).

Currently, most of the challenges related to change management security practices are addressed using tools and technologies (Singh, Picot, Kranz, Gupta, & Ojha, 2013; Volonino & Robinson, 2004; Vaast, 2007). However, Keef (2019) and Herath and Rao (2009) argue that tools and technologies alone are not enough to address the change management security problems just presented. To improve overall change management security 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 objective of this research is to develop a methodology that will effectively address weaknesses identified in traditional SCC assessment methodologies and explore whether such new methodology enhance the overall information security over accounting data in organizations. A methodology that corrects literature-identified weaknesses while is also capable of modelling imprecise parameters when evaluating SCC will result in a more accurate assessment. One technique that can be used to address the limitations stated above is through Fuzzy Set Theory (FST). The remainder of this research paper is organized as follows. Section 2 provides a summary of the literature reviewed related to SCC evaluation and selection. Section 3 explains the theory to be used in the development of the proposed methodology. Section 4 presents the proposed solution approach. Section 5 presents discussion and opportunities for future research, while Section 6 provides conclusions.

Literature Review

Previous Approaches in the 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 list 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.

In Otero (2019a), a research approach was proposed using Grey Systems Theory that quantified the importance of each SCC considering organizations' goals and objectives. In a similar research study, Otero (2019b) developed a quantitative approach to assist management in evaluating SCC using the Analytic Hierarchy Process. Through case evaluations, the above approaches were proven successful in providing a way for measuring the quality of SCC in organizations. However, opportunities for future work were identified that could enhance these approaches in order to improve the overall quality of the SCC selection process. For instance, traditional methodologies nor the solutions described above considered the true degree of relevance (imprecise in nature) when evaluating SCC. The aforementioned still represents a major problem for organizations, potentially impacting the overall security over accounting applications.

The use of baseline manuals or best practice frameworks, according to Barnard and Von Solms (2000), is another approach widely used by organizations to introduce minimum controls in organizations. Based on Saint-Germain (2005), 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 as they leave the choosing of controls to the user, while offering little guidance in determining the best controls to provide adequate protection for the particular business situation (Van der Haar & Von Solms, 2003). Additionally, frameworks do not consider organization specific constraints, such as, implementation costs, 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 accounting 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, 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 and Von Solms, 2003). Furthermore, they do not necessarily take into consideration organization specific constraints, such as costs, scheduling, and resource constraints.

The literature just presented clearly evidences limitations in existing SCC assessment methodologies. It is argued that a methodology based on FST will allow for a more accurate assessment of imprecise parameters than traditional methodologies (Zimmermann, 2010; Otero, Tejay, Otero, & Ruiz, 2012).

Fuzzy Set Theory

Based on Schryen (2010), FST is an uncertainty theory useful in the absence of probabilities and in the presence of subjective assessments. Per Schryen (2010), the idea of FST is “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 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 fuzzy sets can be defined mathematically by assigning a value (representing its grade of membership in the fuzzy set) to each possible individual in the universe of discourse. Such value or 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). 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. Figures 1 and 2 show examples of trapezoidal and triangular fuzzy sets, respectively. Figure 1 denotes SCOPE by a particular SCC as a function of a rating from one to five. Here, ratings of one and four represent the lower and upper bounds, respectively. Ratings of two and three are the lower and upper modal values, meaning that SCC that protect two and three applications will fully belong to the fuzzy set (i.e., higher priority of selection). On the other hand, SCC that do not protect any application (i.e., rating less than one) and those that protect five or more applications, according to Figure 1, will fall outside of this fuzzy set. Similarly, in Figure 2, a triangular fuzzy set denotes RELEVANCE by a particular SCC as a function of a rating from one to 10. A rating of five here 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.

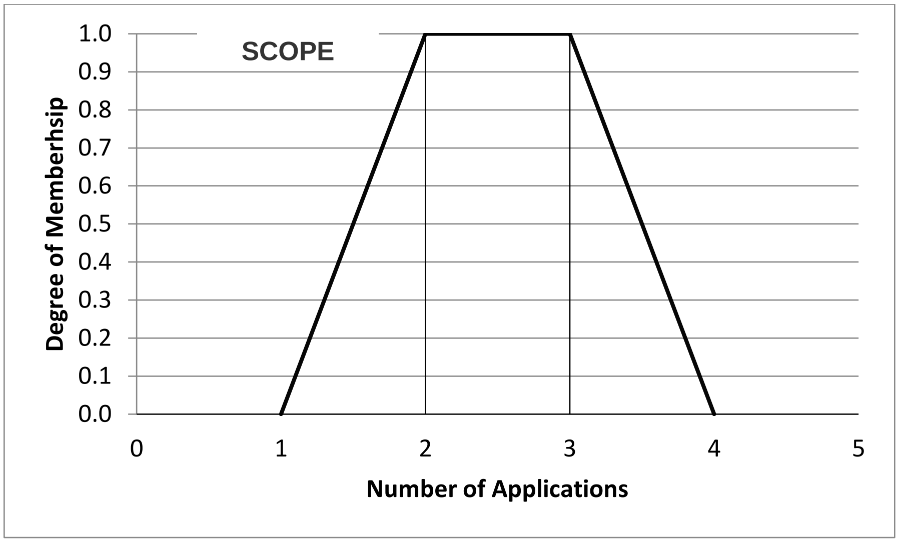


Figure 1. Example of a Trapezoidal Fuzzy Set

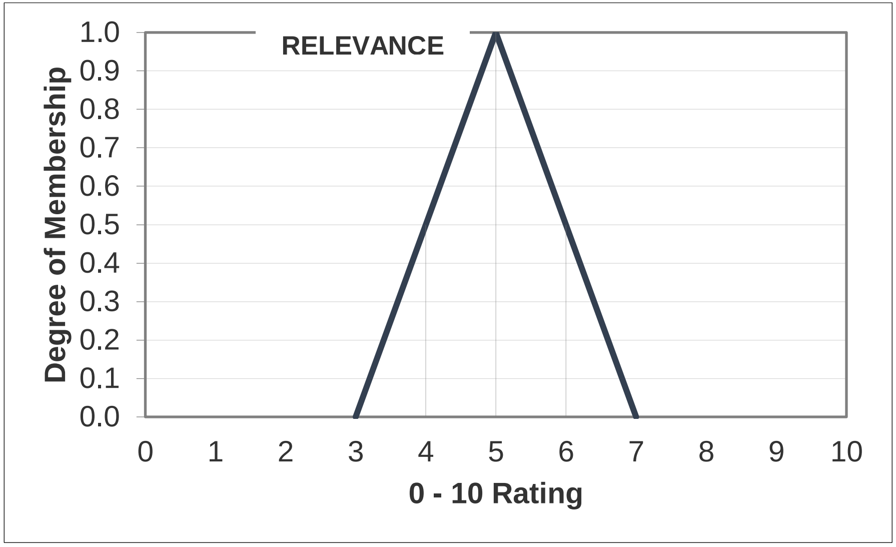


Figure 2. Example of a Triangular Fuzzy Set

As seen, FST provides for various forms of membership functions. Klir and Yuan (1995) state that determining appropriate membership functions is essential for making FST practically useful. Common membership functions used to represent fuzzy numbers include 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.

Fuzzy Reasoning

Based on Das (2009), fuzzy reasoning refers to the process of developing logical inferences from imprecise premises. A very common inference rule used in classical logic is the *modus ponens*, which states that a conclusion can be inferred provided there is 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. Table 1 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*.

Table 1. Classical *Modus Ponens*.

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

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 minimum compositional rule of inference, which provides for a fuzzy conclusion given both, a fuzzy rule and a fuzzy fact, as shown in equation (1).

$$\mu_B(y) = \sup_{x \in X} \min [\mu_A(x), R(x, y)] \tag{1}$$

Klir and Yuan (1995) state that equation (1) obtains degree of membership $\mu_B(y)$ for all $y \in Y$ given a fuzzy implication *R*; as well as degree of membership $\mu_A(x)$ given that *R* is a fuzzy relation on *X* x *Y* and *A* and *B* are fuzzy sets on *X* and *Y*, respectively. With the compositional rule of inference, a fuzzy conclusion can be obtained given both, a fuzzy rule and a fuzzy fact. The generalized *modus ponens* form of inference (shown in Table 2) is considered by many as the foundation for various fuzzy reasoning methods presented in the literature (Mizumoto & Zimmermann, 1982).

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	$\mu_B(y)$

The fuzzy reasoning technique to be used is the Mamdani Max-Min (Mamdani) method, which engages the generalized *modus ponens* just described for each fuzzy rule. When producing output for decision-making, the Mamdani method does so by providing fuzzy, non-linear conclusions obtained provided both fuzzy rules and fuzzy facts. Given the high subjectivity identified in the literature for existing SCC evaluation methods, Mamdani offers organizations advantages when providing for mathematical convenience due to its simplicity and low computational complexity, high degree of accuracy when evaluating imprecision information, and ease of implementation and testing (Klir & Yuan, 1995). According to Petrovic-Lazarevic (2001), another critical advantage of using a rule-based approach such as Mamdani is that processing for all received inputs, via fuzzy 'if-then' rules, is strictly human based. This approach can be expressed in simple language words using the logic a human would use to perform the tasks.

The Mamdani method is the most common fuzzy inference technique (Klir & Yuan, 1995), and it is performed in four steps: (1) Fuzzification of the input variables; (2) Evaluation of rules (inference); (3) Aggregation of the rule outputs (composition); and (4) Defuzzification. The Mamdani method follows the multi-conditional reasoning structure illustrated in Table 3.

Table 3. Multi-conditional Reasoning Structure.

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	$\mu_B(y)$

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 (Petrovic-Lazarevic, 2001). For nonsingleton fuzzy rules and based on operator 'AND', the fuzzy implication is computed as the intersection or conjunction of the statements in the antecedent via the minimum logical operation shown in equation (2).

$$\mu_{A\cap B}(x) = \min\left[\mu A(x), \mu B(x)\right] \quad (2)$$

Equation (2) returns the smallest element where A and B are limited to the range (0, 1). Fuzzy operator 'OR', on the other hand, is known as the fuzzy union or disjunction, returning the maximum elements where again A and B are limited to the range (0, 1). It is denoted by equation (3), where A and B are two given fuzzy sets with memberships functions *μA(x)* and *μB(x)*.

$$\mu_{AUB}(x) = \max\left[\mu A(x), \mu B(x)\right] \quad (3)$$

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. Evaluation criteria for this proposed research study may include change management-related variables such as access controls, incident management, estimated costs, restrictions, scope, risks, and compliance with organization's goals and objectives, among others. These criteria have been defined within well-known international security and change management standards like ISO/IEC 17799, 27001, and 27002 (Saint-Germain, 2005; Da Veiga & Eloff, 2007; ISACA, 2009; Nachin, Tangmanee, & Piromsopa, 2019). Fuzzy sets will be created to represent each of the above variable (or criteria) used to assess and determine ultimate SCC selection. Each criteria will have its own set of fuzzy or inference rules defined to assist with the evaluation. Upon the result of truth values from antecedents, fired rules will be aggregated per criteria, and utilized for final SCC selection inference.

Defuzzification

Defuzzification converts conclusions from fuzzy sets into a real number, or a single crisp value (Yager, 1996). Klir and Yuan (1995) also define the defuzzification process as the conversion of a fuzzy quantity to a precise quantity, represented by the logical union of two or more fuzzy membership functions defined on the universe of discourse of the output variable. In other words, the purpose of defuzzification is to find one single crisp value that summarizes the fuzzy set. Available defuzzification methods include the center of gravity approach (i.e., centroid), which uses integrals to calculate the area of a combination of fuzzy sets, and the common weighted average method. The centroid method takes the center of gravity (COG) and uses integrals to calculate the area of a combination of fuzzy sets. Equation (4) describes the algebraic expression for this method, where μ_A are the degrees of membership. The calculation of the COG is simplified if a finite universe of discourse and thus a discrete membership function is considered. In equation (5), μ_i is the value of the membership function of the fuzzy set rule *i*, A_i is the corresponding area and $\alpha_i$is the degree that the rule *i* is fired (between 0 and 1).

$$COG = \frac{\int_a^b \mu_A(x)x\,dx}{\int_a^b \mu_A(x)\,dx} \tag{4}$$

$$COG = \frac{\sum_{i=1}^{n} \alpha_i \mu_i}{\sum_{i=1}^{n} \alpha_i A_i} \tag{5}$$

The weighted average method, on the other hand, is reliable, less complicated and time consuming, and also used to approximate the center of gravity (Genske & Heinrich, 2009). The weighted average defuzzification method, based on peak values for every fuzzy set, calculates weighted sums of the peak values. Based on those weight values and the degree of membership for fuzzy outputs, crisp values of the output are determined using equation (6), where *μi* is the degree of membership in output singleton *i*, and *Wi* is the fuzzy output weight value for the output singleton *i* (Mizumoto & Zimmermann, 1982; Klir & Yuan, 1995).

$$Z_0 = \frac{\sum \mu(x)_i \times W_i}{\sum \mu(x)_i} \tag{6}$$

Proposed Solution Approach

The proposed solution approach involves a questionnaire that will be provided to key finance and IT personnel within an organization to determine the initial degree of relevance for SCC. Given that most organizations have Accounting and IT departments within their structure, it is stated that the target audience 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 17799 and 27002 standards, which are widely used in organizations to select SCC (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 selecting SCC.

The proposed solution approach will employ FST to create fuzzy sets of crisp rating levels (i.e., 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 one to five (i.e., VL, L, M, H, VH), where higher ratings represent a higher criticality 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 will significantly assist management’s decision-making process in implementing only the most effective SCC in order to protect accounting applications.

For illustration purposes, results from a simulated evaluation using the proposed assessment methodology are shown in Table 4, as applied in the context of a fictitious organization implementing SCC from ISO/IEC 27002, an international cybersecurity management standard. The organizational requirement is to determine (and implement) the most effective SCC in order to protect accounting applications. For evaluation purposes, criteria defined within the ISO/IEC 17799, 27001, and 27002 were referred to. The synthetic or simulated data inputted into the fuzzy inference system model represents real-life operational data from an organization’s finance and IT stand point. Overall, the fuzzy inference system model evaluated 15 SCC against the literature-based criteria mentioned earlier. After the analyses were performed consistent with Section 4, fuzzy logic/reasoning was put to work to ranked SCC by fusing their respective assessment values into a single, quantified measure using the Mamdani Max-Min fuzzy reasoning technique. The unified, crisp scores computed in Table 4 provide organizations with a specific, precise measurement of relevance for each SCC evaluated. The derived relevance measurement can be used as the main metric for ultimately selecting SCC.

Table 4. Simulated SCC Evaluation Using the Proposed FST-based Model.

SCC #	SCC Description	Score
1	Requests for system changes (e.g., upgrades, fixes, emergency changes, etc.) are documented and approved by management before any change-related work is done.	92.63
2	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.	38.10
3	Documentation related to the change implementation has been released and communicated to system users.	45.89
4	Systems for managing passwords should be in place for accounting application systems and should ensure the configuration and implementation of quality passwords.	80.67
5	System changes are tested before implementation into the production environment consistent with test plans and cases.	98.89
6	Inactive sessions should shut down after a defined period of inactivity.	91.25
7	Test plans and cases involving complete and representative test data (instead of production data) are approved by application owners and development management.	78.56
8	Restrictions on connection times should be used to provide security for high-risk applications.	82.77
9	Problems and errors encountered during the testing of system changes are identified, corrected, retested, followed up for correction, and documented.	96.32
10	Sensitive systems should have a dedicated (isolated) computing environment.	34.93
11	Prior to implementation of system changes in live and production environments, of formal acceptance should be obtained supporting that testing has been satisfactorily completed, test results were successful and adequate to prevent tampering, and user requirements were met.	96.23
12	A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.	33.53
13	Personnel independent from those with access to development or test environments review changes and deploy them into the live or production environment.	69.36
14	A network access control policy should be established, documented, and reviewed based on business and security requirements.	97.18
15	Management should review users' access rights within network systems at regular intervals using a formal process.	90.14

For purposes of this illustration, assume that only SCC with scores of 90 and higher are to be selected by the organization consistent with the membership functions defined. This means that SCC 1, 5, 6, 9, 11, 14, and 15 are the ones to be selected by the organization.

Contrary to other approaches and methodologies found in the literature to evaluate SSC (refer to Section 2), the proposed methodology will assist organizations in: (1) addressing the existing weaknesses identified in the literature; (2) 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 relevant change management criteria.

Discussion and Future Research

As seen throughout this research, studies continue to support the harmful effects of unsuccessful and/or weak change management security practices which result in opportunities for fraud, manipulation of information, and computer breaches, among others. Through review of the literature, a critical limitation identified related to current SCC assessment methodologies was that imprecise parameters are being modelled as precise ones. To address this limitation, the development of an innovative 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 will get selected, while maintaining a well-designed, secured, and controlled information system environment.

Klir and Yuan (1995) further stress the flexibility of the fuzzy approach, particularly, when adding more variables to a problem, as it would only require writing new rules or editing the existing ones. The above translates into a lesser amount of effort than rewriting an entire algorithm. Since FST deals with uncertainty, it is a great utility also considered essential to science. FST assists in understanding the phenomenon of reality (be it natural or man-made) via: (1) performing adequate predictions or retrodictions; (2) learning about controlling the phenomenon; and (3) utilizing such capabilities for various other ends.

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 limitations stated above, it is argued that a FST perspective of evaluating SCC is valuable for organizations in safeguarding their accounting applications, as well as when dealing with uncertainty and imprecision.

Future research work could also examine results from the developed approach and from other SCC evaluation methodologies for comparison purposes to determine which method would be the most effective. Another research opportunity would 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. A last research opportunity includes the extension of the proposed approach by refining the questions used in the questionnaire or incorporating additional ones to improve the current investigation.

Conclusion

This research proposes the development of a decision-support methodology, using fuzzy set theory, that can better safeguard accounting applications by allowing for a more robust implementation of SCC. As evidenced, evaluating SCC using fuzzy set theory leads to a more precise assessment, resulting in a more secure financial environment.

The main theoretical contribution of this research is the development of a methodology, anchored by fuzzy set theory, that addresses the limitations identified in the literature for SCC assessment methodologies, and ultimately enhances the overall security of accounting applications in organizations. The methodology developed herein lays down the foundation for the development of a fuzzy expert system as a solution to the existing SCC evaluation and ranking problem. 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 modelling, problem solving, and data mining tool, and has proven superior to existing methods, as well as attractive to enhance classical approaches. FST also 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. Moreover, a FST-based methodology leads to more detailed and thorough assessments, while appropriately modelling human decisions related to SCC evaluation, which are imprecise in nature (Petrovic-Lazarevic, 2001). As a final theoretical contribution, this research has presented opportunities and areas for further related research work.

Regarding practical contributions, the methodology created herein can be implemented in a spreadsheet or software tool and promote usage in practical scenarios where highly complex methodologies for SCC selection are impractical. Moreover, the methodology fuses multiple evaluation criteria to provide a holistic view of the overall quality of SCC, and it is easily extended to include additional evaluation criteria factor not considered within this research. 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. Finally, the methodology provides a mechanism to evaluate the quality of SCC in various domains. Results from this research support that a FST-based methodology will, in fact, assist organizations in evaluating and, thus, determining and selecting only the most effective SCC.

References

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.

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

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.

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

Demicco, R. V., & Klir, G. J. (2004). *Fuzzy logic in geology* (1st ed.). Academic Press.

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.

Federal Bureau of Investigation. (2019). *White-Collar Crime. FBI Major Threats & Programs*. What We Investigate. https://www.fbi.gov/investigate/white-collar-crime.

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

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

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.

ISACA. (2009). *COBIT and Application Controls: A Management Guide*. ISACA.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2004). Information systems security policies: A contextual perspective. *Computer Security, 24*(1), 246-260.

Keef, S. (2019). *Why Security Product Investments Are Not Working*. ISACA Journal. https://www.isaca.org/Journal/archives/2019/Volume-2/Pages/why-security-product-investments-are-not-working.aspx

Klir, G. J., & Yuan, B. (1995). *Fuzzy Sets and Fuzzy Logic: Theory and Applications*. Upper Saddle River, NJ: Prentice Hall PTR.

Lavion, D. (2018). *Pulling fraud out of the shadows: Global Economic Crime and Fraud Survey 2018*. PricewaterhouseCoopers LLP. https://www.pwc.es/es/publicaciones/deals/assets/encuesta-mundial-fraude-delito-economico-2018.pdf

Mizumoto, M., & Zimmermann, H. J. (1982). Comparison of fuzzy reasoning methods. *Fuzzy Sets and Systems, 8*(3), 253-283.

Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). *How to increase cybersecurity awareness*. ISACA Journal. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/how-to-increase-cybersecurity-awareness

Otero, A. R. (2019a). Optimization methodology for change management controls using GST. *International Journal of Business and Applied Social Science, 5*(6), 41-59.

Otero, A. R. (2019b). System change controls: A prioritization approach using AHP. *International Journal of Business and Applied Social Science, 5*(8), 56-68.

Otero, A. R. (2015a). Impact of IT auditors' involvement in financial audits. *International Journal of Research in Business and Technology, 6*(3), 841-849.

Otero, A. R. (2015b). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems, 18*(1), 26-45.

Otero, A. R. (2018). *Information technology control and audit* (5th ed.). Boca Raton, FL. CRC Press and Auerbach Publications.

Otero, A. R. (2014). *An information security control assessment methodology for organizations* (Doctoral dissertation). Nova Southeastern University, Fort Lauderdale, USA. Retrieved from

NSUWorks, Graduate School of Computer and Information Sciences. (266) https://nsuworks.nova.edu/gscis_etd/266

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.

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

Otero, A. R., Sonnenberg, C., & Bean, L. (2019). Quality assessment of access security controls over financial information. *International Journal of Network Security & Its Applications, 11*(6), 1-18.

Pedrycz, W. (1994). Why triangular membership functions? *Fuzzy Sets & Systems, 64*(1), 21-30.

Petrovic-Lazarevic, S. (2001). Personnel selection fuzzy model, *International Transactions in Operational Research. 8*(1), 89-105.

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

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Salkind, N. J. (2009). *Exploring research* (7th ed.). Upper Saddle River, NJ: Prentice-Hall, Inc.

Schryen, G. (2010). A fuzzy model for IT security investments. *Proceedings of Sicherheit*, Schutz und Zuverlässigkeit, 289-304.

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.

The Institute of Internal Auditors. (2012). *Global Technology Audit Guide 2: IT change management: Critical for organizational success* (3rd ed.). https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Global-Technology-Audit-Guide-IT-Change-Management-Critical-for-Organizational-Success.aspx

The Institute of Internal Auditors. (2019). *Global Technology Audit Guide 8: Auditing Application Controls*. https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG8.aspxs

Thome, 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.

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.

Van der Haar, H., & Von Solms, R. (2003). A model for deriving information security controls attribute profiles. *Computers & Security, 22*(3), 233-244.

Volonino, L., & Robinson, S. R. (2004). *Principles and practice of information security* (1st ed.). Upper Saddle River, NJ: Pearson Prentice Hall, Inc.

Yager, R. R. (1996). Knowledge-based defuzzification. *Fuzzy Sets Systems, 80*(1), 177-185.

Zadeh, L. (1965). Fuzzy sets. *Information Control, 8*(1), 338-353.

Zimmermann, H. -J. (2010), Fuzzy set theory. WIREs Comp Stat, 2: 317-332. doi:10.1002/wics.82