International Journal of Business and Applied Social Science

EISSN: 2469-6501
VOL: 5, ISSUE: 6
JUNE/2019
DOI: 10.33642/ijbass.v5n6p4
https://ijbassnet.com/

©Center for Promoting Education and Research www.cpernet.org

Optimization Methodology for Change Management Controls Using Grey Systems Theory

Angel R. Otero
Nathan M. Bisk College of Business
Florida Institute of Technology
150 West University Blvd.
Melbourne, FL 32901
Office: 321-674-8782
Email: aotero@fit.edu
USA

Abstract

General information technology controls include controls related to information systems that must be adequately designed and implemented to support critical business processes. They commonly include controls over change management (i.e., system change controls) and ensure the effective implementation of changes in the information technology environment. Alarming facts within the literature point to inadequacies in change management practices, particularly the evaluation of system change controls in organizations. Research efforts have resulted in various methodologies developed to tackle the assessment of system change controls. Nevertheless, these methodologies identify weaknesses that can prevent an effective assessment and, ultimately, adequate selection of those controls. This research proposes a novel approach using Grey Systems Theory that quantifies the importance of each system change control considering organizations' goals and objectives. Through a case study, the approach is proven successful in providing a way for measuring the quality of system change controls based specifically on organizations' criteria.

Keywords: Change management, system change controls, information security, grey systems theory, assessment

1. Introduction

Today, more than ever, the dependence and exposure of information systems are significantly high, constantly threatening perhaps the most valuable asset in an organization, its information. Protection of such information from constant attacks, as well as compliance with new and existing laws and regulations, have significantly shifted the focus of internal controls in organizations. Organizations now require internal controls to be adequately designed and implemented in order to support critical business processes (Lavion, 2018), as well as mitigate the risks that could prevent them from achieving business objectives (Deloitte, 2018; GTAG 8, 2009).

Common objectives, such as the effectiveness and efficiency of operations, compliance with applicable laws and regulations, and reliability of the entity's financial reporting are being constantly jeopardized in the organization (Otero, 2018; Otero, Ejnioui, Otero, & Tejay, 2011). Effective internal controls should be implemented and frequently monitored in order to ensure the objectives above are achieved and, not less important, security concerns are reduced or eliminated (Otero, Tejay, Otero, & Ruiz, 2012).

As part of the process for assessing the effectiveness of internal controls, particularly, over financial reporting, organizations need to consider controls related to the information systems that support relevant financial processes. These controls are collectively known as general information technology (IT) controls or GITC. GITC assist in the effective development and maintenance of applications; as well as protect business operations by securing the integrity, completeness, and reliability of financial information (Deloitte, 2018; Otero, 2015). GITC provides a basis for relying on the reports and data from applications, and for concluding that automated controls (controls configured within the application) also operate as expected. GITC refers to policies, processes, procedures, and/or activities performed within the IT environment to support the effective operation of application systems, the integrity of reports being generated from those systems, and the overall security. Ineffective GITC, if not timely addressed, may impact the overall functioning of internal controls, result in increased audit costs, and prevent organizations from generating complete and accurate financial reports, ultimately affecting the reputation and brand of the organization (Masli, Richardson, Watson, & Zmud, 2016; Krishnan & Visvanathan, 2007).

GITC commonly include controls over (1) information systems operations; (2) access security; and (3) change management. Change management is a process that ensures the effective implementation of changes in an IT environment (Otero, 2018). It affects relevant technology elements within the organization's IT environment (i.e., application systems, databases, operating systems, and networks) and includes controls around the areas of system software acquisition; change and maintenance; program change; and application system acquisition, development, and maintenance. Change management controls are also known as system change controls (SCC).

SCC help minimize the likelihood of disruption and unapproved changes as well as errors (ITIL, 2016). Examples of typical SCC include the review, testing, and approval of upgrades or releases to applications, databases, and network infrastructure; documentation and approval of system change requests, emergency changes, etc. Given the significance of the activities described above with business processes, organizations must implement SCC in order to maintain the completeness and accuracy of the information, as well as the reliability of the business processes. SCC is critical in ensuring the security, integrity, completeness, and reliability of the business process, including financial information (Keef, 2019; GTAG 2, 2012; Ejnioui, Otero, Tejay, Otero, & Qureshi, 2012).

1.1 Challenges with the Change Management Process

Changes in the IT environment, including systems and applications, can result from a new law or regulation requirement, or from an update needed to enhance the current system's functionality (Masli et al., 2016). In both of these cases, before implementation in the live or production environment, changes must be evaluated, documented, approved, developed, and tested in an adequate and controlled manner (Hornstein, 2015; Mitra & Mishra, 2016). However, there are always several challenges when carrying out this process.

For instance, implementation of changes directly into an application system may override already existing automated application controls for particular financial transactions or a certain set of transactions, leading to serious data accuracy and integrity issues. An example would be the direct implementation of a change that affects the system's calculation of depreciation for recorded fixed assets. The direct change may have not been adequately tested or evaluated, resulting in an inaccurate posting of depreciation. Moreover, if this change is implemented by year end, it may lead to an incorrect representation of financial information. Another example would be the direct implementation of emergency changes. According to Pillai, Pundir, and Ganapathy (2014), an emergency change is any change, major or minor, that must be addressed quickly as an immediate fix, without following standard change management procedures (e.g., appropriate documentation, rigorous testing, etc.) prior to implementation in production. Management must approve such changes before they are undertaken or implemented. These types of direct changes are typically not documented or tested prior to their implementation, leading to an adverse impact which would be difficult to roll-back and trail.

Another challenge in the change management process involves the implementation of unauthorized changes which may harm the production environment, causing severe data integrity issues. Unauthorized changes may lead to incomplete implementations, leaving out critical functionality. Unauthorized changes may also result in the processing of incorrect business data, ultimately opening up opportunities for fraud (Lavion, 2018). Proper authorization of changes prior to their development and implementation will bring all relevant stakeholders on board, and ensure that the intended change is aligned and consistent with business goals, objectives, and/or requirements.

A third challenge relates to the inadequate segregation of duties. A well-controlled change management process monitors and ensures that there is proper segregation between who initiates the change, who approves the change, who develops the change, and who implements the change in the production environment. Having the same individual with granted access to analyze, design, construct, test, and implement a change in the live environment may result in overlooking errors, implementing incorrect and incomplete changes, etc. Per Otero (2018), individuals with complete access to develop and implement changes into production will trigger many dangerous systems' risks, including but not limited to: unauthorized access to programs or data; unauthorized remote access; inaccurate information; erroneous or falsified data input; incomplete, duplicate, and untimely processing; communications system failure; inaccurate or incomplete output; and insufficient documentation. Segregation of duties certainly plays an important role in the entire change management process and must be effectively controlled.

1.2 Current State of the IT Environment

Schwartz (1990) states that losses of confidential and sensitive financial information will continue to happen and their effect will be devastated to organizations. According to the American Institute of Certified Public Accountants (AICPA), cybercrime's global cost (including losses related to financial information) is estimated to reach $6 trillion by 2021 (Morgan, 2017). The AICPA also states that organizations are no longer immune, and attacks on their financial information are not a matter of if, but when. Examples of such attacks on information (e.g., corporate fraud, etc.) 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).

Based on the Federal Bureau of Investigation's (FBI) (2019), corporate fraud continues causing extensive damage to the U.S. economy and investor confidence. Examples of this type of fraud, per FBI (2019), involve accounting schemes like posting false accounting entries; misrepresenting the current financial condition; performing fraudulent trades designed to inflate profits or hide losses; and/or injecting illicit transactions designed to evade regulatory oversight. The above schemes, as expected, are designed to deceive investors, auditors, and analysts about the true financial condition of the company. Through the manipulation of financial data, share price, or other valuation measurements, the financial performance of a company may remain artificially inflated based on fictitious performance indicators provided to the investing public. To add to the above, the use of web applications (which has grown exponentially in the recent years) has added more security risks and vulnerabilities around financial information creating significant exposure for many organizations (ISACA, 2011; Thomé, Shar, Bianculli, & Briand, 2018). For example, in May 2019, accounting firms and clients realized that a popular cloud-based tax and accounting software had been compromised and were ultimately shut down as a result of a malware attack (Ryan, 2019).

The facts and figures above are very alarming to say the list. They point to inadequacy in today's IT environment and, most importantly, serve as motivation for finding new ways to help organizations improve their capabilities for securing, managing, and controlling valuable information. An example of such a "new way" is the implementation of adequate and effective change management security practices. At present, most of the challenges seen related to change management security practices are being addressed with software tools and technologies (Singh, Picot, Kranz, Gupta, & Ojha, 2013; Volonino & Robinson, 2004; Vaast, 2007). Nevertheless, Keef (2019) and Herath and Rao (2009) argue that software tools and technologies alone are not sufficient to address the change management security problems just described. To improve overall change management security practices, organizations must identify new methods to protect their sensitive and critical information. One of those methods is through the effective assessment (and further implementation) of SCC to maintain a well-designed and controlled information system environment (Barnard & Von Solms, 2000; Da Veiga & Eloff, 2007; Karyda, Kiountouzis, & Kokolakis, 2004). Change management is at its best in organizations when only the most appropriate SCC are implemented. The reality is that, due to a variety of organizational-specific constraints (e.g., cost, scheduling, resources availability, etc.), organizations do not have the luxury of implementing all required SCC. Therefore, the selection of SCC within organizations' business constraints become a non-trivial task.

Based on the literature reviewed (refer to Section 2), traditional change management evaluation methodologies do not promote an effective assessment and prioritization SCC in organizations. For instance, most evaluation and selection methods of SCC in organizations use crisp or dichotomous values. This means that organizations perform their selection based on whether the SCC is relevant or not, and not necessarily considering the degree of such relevance or significance for each SCC. 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.

The aim of this research is to develop an assessment methodology, based on Grey Systems Theory (GST), that will adequately address the weaknesses identified in traditional SCC assessment methodologies, resulting in a more accurate selection of SCC. It is argued that an SCC assessment methodology based on GST will consider imprecise parameters (in the form of organizations' criteria) when evaluating SCC, and will quantify and rank such (relevance) parameters using real numbers. Development of such a methodology not only results in a more effective and precise selection of SCC but constitutes a significant contribution to the change management security 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 presents the results of an SCC evaluation/prioritization case study using the proposed approach. Section 5 discusses contributions and opportunities for future research, while Section 6 provides a summarized conclusion.

2. Literature Review

Organizations are required to identify and implement appropriate controls to ensure adequate information security (Saint-Germain, 2005). 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). Following is a detailed description of the approaches and methodologies that have been used in organizations to assess and select SCC.

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

Barnard and Von Solms (2000) stress the challenge that it has been for organizations to identify and select the most effective SCC, including the many attempts 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.

Nonetheless, RAM 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 RAM, organizations may identify 25 change management-related risks. However, 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. Dhillon and Torkzadeh (2006) state that organizations, when performing RAM, establish controls that are either unnecessary or relate to trivial issues. Furthermore, exclusive reliance on RAM has often been criticized since it has proven to be more problematic for maximizing information security rather than beneficial. 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), Information Technology Infrastructure Library (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 (CMM).

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 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 to name a few. 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.

Another method used to identify and select SCC in organizations has been through checklists. Chen and Yoon (2010) used checklists as a framework to identify common SCC, including information security risks, within cloud-based organizations. The checklists were to be used by both, internal and external auditors, in assuring a secure computing environment. Chen and Yoon (2010) completed checklists for the Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) delivery service models within a public cloud. Numerous information security checklists have been proposed and used over the years (Baskerville, 1993). Their importance, according to Dhillon and Torkzadeh (2006), has been focused on identifying "all possible threats to a computer system and propose solutions that would help in overcoming the threat" (p. 294). Nonetheless, Dhillon and Torkzadeh (2006) stress that the significance of information security checklists has declined simply "because they provide little by way of analytical stability" (p. 294). Based on interviews by Dhillon and Torkzadeh (2006) performed on information security managers, checklists are not considered to be the essence of information security. Even though checklists may be viewed as good means to ensure information security, exclusive reliance on them could result in a flawed information systems security strategy (Dhillon & Torkzadeh, 2006). Furthermore, Backhouse and Dhillon (1996) argue that although checklists draw concern on particular details of procedures, they do not completely address the key task of understanding the substantive questions. Checklists are concerned with what can be done without any analytical stability in regards to the kind of actions identified (Baskerville, 1993).

In Otero, Otero, and Qureshi (2010), innovative control evaluation and selection approach were developed, particularly for information security controls, to help decision makers select the most effective ones in resource-constrained environments. The approach used desirability functions to quantify the desirability of each security control after taking into account the benefits and restrictions associated with implementing the particular control. The above-provided management with a measurement that was representative of the overall quality of each security control based on organizational goals. Through a case study, the approach proved successful in providing a way for measuring the quality of security control in organizations. Otero et al.'s (2010) methodology took into consideration relevant quality attributes of each security control in order to determine their relative importance. This allowed a control selection scheme that represented how well these security control met quality attributes, and how important those quality attributes were for the specific organization. The quality attributes were defined in terms of different features, where each feature was determined by the organization to either be present or not. Once all features were identified, each individual security control was evaluated against each feature using a simple binary (boolean) scale (0 or 1). Security controls that satisfied the highest number of features exposed a higher level of quality (or priority) for that particular quality attribute. The above resulted in a control evaluation approach based on how well security controls met quality attributes, and how important those quality attributes were for the organization. However, boolean criteria for evaluating the quality attributes of each security control in order to ultimately determine which ones to select, may not be considered a precise enough assessment for selecting and ultimately implementing security controls in organizations.

Based on the reviewed literature, there have been no other studies that have addressed the evaluation of change management security controls or SCC in organizations. Table I summarizes the literature review presented, pointing out the weaknesses from the above control assessment methodologies. The above literature evidence weaknesses and inadequacies in existing assessment methodologies for SCC in organizations. A methodology that addresses or enhances the above weaknesses and inadequacies has yet to be proposed in the change management security literature. To properly evaluate the quality, importance, and priority of SCC in organizations, management must follow a methodology that takes into consideration the quality attributes and the features of SCC that are considered relevant. The methodology must provide capabilities to determine the relative importance of each identified feature. This would allow the methodology to provide an SCC selection scheme that represents how well these SCC meet quality attributes and their features, and how important those features are for the specific organization. To achieve this, a methodology using GST to solve a multi-attribute decision problem is proposed. First, a set of quality attributes is identified as evaluation criteria for all possible SCC. These attributes are defined in terms of different features, where the importance of each feature is expressed as a grey number. SCC that satisfy the highest number of features would expose a higher level of quality for that particular quality attribute. Once all SCC are evaluated and measurements computed for all features, the proposed approach uses the Euclidian distance between each SCC implementation and the ideal SCC to fuse all measurements into one unified value that is representative of the overall quality of the SCC. The resulting ranking of each SCC is derived based on the goals and specific needs of the organization. The next section will discuss the theory that will serve as the basis for developing the proposed assessment approach.

Table I: Weaknesses of literature-based SCC assessment methodologies

SCC Assessment Methodology	Description of Weakness/Inadequacy
1. Risk Analysis and Management (RAM) (Barnard & von Solms, 2000; Dhillon & Torkzadeh, 2006)	- RAM has been described as a subjective, bottom-up approach (Van der Haar & Von Solms, 2003), not taking into account specific organizations' constraints (Barnard & von Solms, 2000).

	- When organizations perform RAM, controls that are either unnecessary or relate to trivial issues may be implemented (Dhillon & Torkzadeh, 2006). - Exclusive reliance on RAM has proven to be more problematic than beneficial for maximizing information security (Dhillon & Torkzadeh 2006).
2. Baseline Manuals or Best Practice Frameworks (COBIT, ITIL Change Control, NIST, OCTAVE, ISO / IEC 177995, ISO/IEC 27001 and 27002, and CMM) (Barnard & von Solms, 2000; Saint-Germain, 2005; Da Veiga & Eloff, 2007)	- Baseline manuals or best practice frameworks leave the identification of SCC to the user, while offering little guidance in determining the best SCC to provide adequate security for the particular business situation (Van der Haar & Von Solms, 2003). - Baseline manuals or best practice frameworks do not necessarily account for organization specific constraints, such as, costs of implementation, scheduling, and resource constraints, among others (Barnard & von Solms, 2000).
3. Ad Hoc or Random Approach (Barnard & von Solms, 2000)	- Ad hoc or random approaches lead to the inclusion of unnecessary SCC and/or exclusion of required SCC (Barnard & von Solms, 2000).
4. Legal Requirements Determination Model (Gerber & von Solms, 2008)	- Baseline manuals or best practice frameworks leave the identification of SCC to the user, while offering little guidance in determining the best SCC to provide adequate security for the particular business situation (Van der Haar & Von Solms, 2003). - Baseline manuals or best practice frameworks do not necessarily account for organization specific constraints, such as, costs of implementation, scheduling, and resource constraints, among others (Barnard & von Solms, 2000).
5. Checklists (Chen & Yoon, 2010; Dhillon & Torkzadeh, 2006; Baskerville, 1993; Backhouse & Dhillon, 1996)	- Dhillon and Torkzadeh (2006) stress that the significance of checklists has declined simply "because they provide little by way of analytical stability" (p. 294). - Exclusive reliance on checklists could result in a flawed information systems security strategy (Dhillon & Torkzadeh, 2006). - Checklists do not completely address the key task of understanding the substantive questions (Backhouse & Dhillon, 1996). - Checklists are concerned on what can be done without any analytical stability in

	regards to the kind of actions identified (Baskerville, 1993).
6. Desirability Functions (Otero et al., 2010)	- A boolean criteria for evaluating the quality attributes of security controls in order to ultimately determine which ones to select may not be considered a precise enough (less-subjective) assessment for selecting security controls in organizations (Otero et al., 2010).

3. Theoretical Basis

3.1 Grey Systems Theory

Based on Liu and Lin (2011), GST has significantly contributed to the areas of grey algebraic systems, grey equations, grey matrices, etc.; sequence operators and generation of grey sequences; system analysis based on grey incidence spaces and grey clustering; grey prediction models; decision making using grey target decision models; and optimization models using grey programming, grey game theory, and grey control.

In practical applications, a grey number represents an indeterminate number that takes its possible value from an interval or a set of numbers. The symbol ⊗ denotes a grey number. Basic types of a grey number, according to Liu and Lin (2011), are based on the following definitions:

Definition 1. Let $\otimes x = [\underline{x}, \overline{x}] = \{x | \underline{x} \leq x \leq \overline{x}, \underline{x} \in \mathbb{R} \text{ and } \overline{x} \in \mathbb{R}\}$. Then, $\underline{x}$ and $\overline{x}$ are the lower and upper limits of the grey number $\otimes x$, respectively (Lin, Lee, & Chang, 2008).

Definition 2. Let $\otimes x$ be as defined in Definition 1, then (Yamaguchi, Li, Mizutani, Akabane, Nagai, & Kitaoka, 2006):

- If $\underline{x} \rightarrow -\infty$ and $\overline{x} \rightarrow \infty$, then $\otimes x$ is called a black number, meaning that the data have no information.
- If $\underline{x} = \overline{x}$, then $\otimes x$ is called a white number, meaning that the data have complete information.
- If $\otimes x = [\underline{x}, \overline{x}]$, then $\otimes x$ is called a grey number, meaning that the data have incomplete or uncertain information.

Definition 3. If k is a positive real number, then $k \times \otimes x = k \times [\underline{x}, \overline{x}] = [k\underline{x}, k\overline{x}]$ can be called the number product of k and $\otimes x$.

Definition 4. Let $L_p(\otimes x, \otimes y)$ denote the grey number Minkowski distance, then $L_p(\otimes x, \otimes y)$ can be defined as (Rui & Wunshch, 2005):

$$L_p(\otimes x, \otimes y) = \frac{1}{\sqrt[p]{2}} \sqrt[p]{\left(|\overline{x} - \overline{y}|^p + |\underline{x} - \underline{y}|^p\right)}, p > 0 \qquad (1)$$

Definition 5. Let $\otimes x = [\otimes x_1, \otimes x_2, \dots, \otimes x_m]$ and $\otimes y = [\otimes y_1, \otimes y_2, \dots, \otimes y_m]$ be two m-attribute grey number vectors, the weighted grey number Minkowski distance between $\otimes x$ and $\otimes y$ is defined as (Lin et al., 2008; Rui & Wunshch, 2005):

$$L_p(\otimes x, \otimes y) = \frac{1}{\sqrt[p]{2}} \sqrt[p]{\sum_{j=1}^{m} w_j \left(|\overline{x}_j - \overline{y}_j|^p + |\underline{x}_j - \underline{y}_j|^p \right)} \quad (2)$$

where wj is the weight of the jth attribute.

3.2 Grey Relational Analysis in Multi-Attribute Decision Making

Multi-attribute decision-making problems occur in situations where a finite set of alternatives need to be evaluated according to a number of criteria or attributes. The evaluation consists of selecting the best alternative or ranking the set of alternatives based on those attributes. However, many decision problems present data that is imprecise or ambiguous leading to conflicting situations in which the evaluation of alternatives becomes difficult. This is the case when implementing SCC in organizations. In the past, this information uncertainty has been modeled using fuzzy sets (Klir & Yuan, 1995) or grey numbers (Liu & Lin, 2011). While the former has been around for some time, only recently has interest been growing in the latter, since uncertainty can be modeled and manipulated in more flexible ways using grey number systems than fuzzy sets (Liu & Lin, 2011).

3.3 Selection of SCC

The first step involves identifying a set of SCC that could be implemented in the organization. These SCC can be obtained from the best practice frameworks listed in Section 2. For instance, ITIL Change Control, COBIT, and/or ISO/IEC 27001 and 27002, all offer best practices or controls to help organizations ensure that all program/system changes are appropriately managed, minimizing the likelihood of disruption, unauthorized alterations, and errors which may impact the accuracy, completeness, and valid processing and recording of financial information. Once selected, the SCC is captured in the SCC vector I as:

$$I = \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_n \end{bmatrix} \quad (3)$$

3.4 Attributes and Features

When planning to implement SCC, it is often necessary to address attributes and features important in the decision problem. Each SCC implementation can be evaluated against a set of quality attributes. The evaluation process takes place as follows. First, each attribute is defined in terms of *f* features, where *f* > 1. Because of the uncertain nature of data, the evaluation of each feature is represented as a grey number. For example, SCC can be evaluated based on the *Scope* attribute. In other words, SCC that effectively minimize the likelihood of disruption, unauthorized alterations, and errors impacting the accuracy, completeness, and validity of processing and recording of financial information in more than one system have a higher priority than SCC that address the above in only one system. In this case, the quality attribute *Scope* can be defined with the following features: *System* 1, *System* 2, ..., *System n*. Therefore, the most important SCC (based on the *Scope* quality attribute) would be one where *System* 1, *System* 2, and *System n* has higher evaluation values. Similarly, the least important SCC based on the *Scope* quality attribute is one where *System* 1, *System* 2, and *System n* have lower evaluation values. As a result, the overall assessment of the *n* SCC based on all *m* features of all quality attributes is captured using the following decision matrix *X*:

$$X = \begin{bmatrix} [\underline{x}_{11}, \overline{x}_{11}] & [\underline{x}_{12}, \overline{x}_{12}] & \cdots & [\underline{x}_{1m}, \overline{x}_{1m}] \\ [\underline{x}_{21}, \overline{x}_{21}] & [\underline{x}_{22}, \overline{x}_{22}] & \cdots & [\underline{x}_{2m}, \overline{x}_{2m}] \\ \vdots & \vdots & & \vdots \\ [\underline{x}_{n1}, \overline{x}_{n1}] & [\underline{x}_{n2}, \overline{x}_{n2}] & \cdots & [\underline{x}_{nm}, \overline{x}_{nm}] \end{bmatrix}$$

(4)

where the rows represent alternatives considered in SCC implementation while the columns represent the attribute features of the same problem. Note that the $\underline{x}_{ij}$ and $\overline{x}_{ij}$ represent respectively the lower and upper bounds of grey number evaluation x_{ij} for $i = 1, 2, .., n$ and $j = 1, 2, .., m$.

3.5 Feature Weights

In general, an SCC feature will be characterized by a very specific goal. For example, the goal of an alternative may consist of minimizing restrictions while maximizing the rest of the SCC features. Optimization goals consist mostly of minimizing or maximizing one or more features associated with a given decision problem. However, these goals may not have the same importance in some cases. To assess the relative importance of each feature, the following weight vector W is created:

$$W = [w_1\ w_2\ \cdots\ w_m]$$

(5)

where wj represents the importance of feature fj. These weights can be decided by one or more experts in a subjective manner or synthesized objectively from the matrix X. In this research, weights are synthesized from the decision matrix using the concept of statistical variance. In contrast to other approaches for synthesizing weights such as the entropy method (Jee & Kang, 2000; Shanian & Savadogo, 2006), the statistical variance is effective and easy to implement (Rao & Patel, 2010). Unlike statistical analysis where the focus is placed on the extremes, variance examines how data points are scattered around the mean. As such, variance provides useful information about how important an attribute is to a decision problem.

Definition 6. Let $\otimes x = [\underline{x}, \overline{x}]$ be a grey number with $\underline{x} < \overline{x}$. If $\otimes x$ is continuous, then,

$$\hat{x} = \frac{1}{2}(\underline{x} + \overline{x})$$

(6)

is the core of $\otimes x$ (Liu & Lin, 2011).

The cores of all grey numbers in the matrix X can be used to compute the weights from X using statistical variance as follows:

$$v_j = \frac{1}{n}\sum_{i=1}^{n}\left(\hat{x}_{ij} - \bar{x}_j\right)^2 \tag{7}$$

where $\hat{x}_{ij}$ is the core of grey number $\otimes x_{ij}$ while $\bar{x}_j$ is the statistical mean of the cores of all grey numbers in feature f_j. The synthetic weight of feature f_j can be computed as follows:

$$w_j = \frac{v_j}{\sum_{k=1}^{m} v_k} \tag{8}$$

for $j = 1, 2, \ldots, m$.

3.6 Normalization of the Decision Matrix

Because of the incommensurability of the values in matrix X, the matrix needs to be normalized. This normalization can be performed as follows (Lin et al., 2008; Chang, 2000):

$$\otimes r_{ij} = \frac{\otimes x_{ij}}{\max\limits_{1\le i\le n} \bar{x}_{ij}} = \left[\frac{\underline{x}}{\max\limits_{1\le i\le n} \bar{x}_{ij}}, \frac{\bar{x}}{\max\limits_{1\le i\le n} \bar{x}_{ij}}\right] \tag{9}$$

$$\otimes r_{ij} = -\frac{\otimes x_{ij}}{\min\limits_{1\le i\le n} \underline{x}_{ij}} + 2 = \left[\frac{-\underline{x}}{\min\limits_{1\le i\le n} \underline{x}_{ij}} + 2, \frac{-\bar{x}}{\min\limits_{1\le i\le n} \underline{x}_{ij}} + 2\right] \tag{10}$$

where equation (9) is applied to maximization features (i.e., the larger-the-better type) while equation (10) is applied to minimization features (i.e., the smaller-the-better-type). The obtained matrix will be the normalized matrix R.

3.7 The Ideal SCC Implementation

Assume that k features in the R matrix are maximization type while the remaining (m–k) features are minimization type. The ideal SCC implementation, also known as the reference sequence in relational analysis, in R can be defined per Zhang, Wu, and Oslon (2005) as:

$$r_0 = [r_{01}, r_{02}, \dots, r_{0m}]$$

(11)

where:

$$r_{0j} = \max_{1 \le i \le n} \overline{r}_{ij}, j \in \{1, 2, \dots, k\}$$

(12)

and:

$$r_{0j} = \min_{1 \le i \le n} \underline{r}_{ij}, j \in \{k+1, k+2, \dots, m\}$$

(13)

In principle, r_0 is regarded as a hypothetical vector of features in which the evaluation values are the optimal values in *R*. However, the evaluation values of each SCC alternative in *R* can be higher in some features while lower in others. As a result, a compromise SCC implementation must be found in *R* that is as close as possible to the ideal implementation.

3.8 Distance Between the Ideal SCC and the SCC Implementations in the Matrix

Equation (2) can be used to compute the Minkowski distance between the ideal SCC and each SCC implementation in the *R* matrix as follows:

$$L_p(r_0, \otimes r_i) = \frac{1}{\sqrt[p]{2}} \sqrt[p]{\sum_{j=1}^{m} w_j \left(|r_{0j} - \overline{r}_{ij}|^p + |r_{0j} - \underline{r}_{ij}|^p \right)}$$

(14)

For practical purposes, it is often suggested to make $p = 2$ thus reducing, in a manner similar to the TOPSIS technique, the Minkowski distance in equation (14) to the Euclidian distance in equation (15) (Lin et al., 2008; Yoon & Hwang, 1985):

$$L_2(r_0, \otimes r_i) = \frac{1}{\sqrt{2}} \sqrt{\sum_{j=1}^{m} w_j \left(\left(r_{0j} - \overline{r}_{ij}\right)^2 + \left(r_{0j} - \underline{r}_{ij}\right)^2 \right)}$$

(15)

3.9 Grey Relational Grade

The grey relational grade of the *i*th SCC implementation can be computed as follows (Yamaguchi, Li, & Nagai, 2005):

$$g_i = \frac{\max\limits_{1\leq i\leq n}\left(L_2(r_0,\otimes r_i)\right) - L_2(r_0,\otimes r_i)}{\max\limits_{1\leq i\leq n}\left(L_2(r_0,\otimes r_i)\right) - \min\limits_{1\leq i\leq n}\left(L_2(r_0,\otimes r_i)\right)} \quad (16)$$

for i = 1, 2, …, n. This grade measure is a scaled ratio of the distance between a given SCC implementation and the two extremes of the ideal SCC. As this grade increases, so does the distance between the SCC implementation and the maximum point of the ideal SCC, thus allowing the SCC implementation to be somewhat not too far from the minimum point of the ideal SCC. Such SCC implementation is highly desirable than one that is located a far greater distance from the maximum or minimum points of the ideal SCC. By sorting the SCC implementations from highest to lowest grey relational grades, we can obtain a ranking of the SCC from best to worst.

4. Case Study

This section presents the results of an SCC evaluation/prioritization case study using the proposed approach. The case study evaluates 10 SCC based on the following identified quality attributes defined within the ISO/IEC 177995 and 27002 standards (Da Veiga & Eloff, 2007; Nachin, Tangmanee, & Piromsopa, 2019; and ISACA, 2009).

1. *Restrictions*–There are restrictions that management must take into account before selecting and implementing SCC. These may include whether the costs involved in the selection and implementation of the SCC are high, whether resources are not available, and whether there are scheduling constraints associated with implementing the SCC. The presence of any of the above will negatively affect the specific quality attribute. That is, SCC with all features present will result in a lower priority; conversely, SCC with all features missing will result in a higher priority. A high priority scenario will be one where the implementation cost of the specific SCC is considered adequate/manageable (e.g., within budget), resources are available to implement the particular SCC, and there are no restrictions in terms of scheduling the SCC (i.e., the SCC can be scheduled anytime during the year). Restrictions are defined as Costs (C), Availability of Resources (AoR), and Scheduling (T).

2. *Scope*–This quality attribute assesses the impact of the SCC on the organization. SCC that effectively minimize the likelihood of disruption, unauthorized alterations, and errors which impact the accuracy, completeness, as well as validity of processing and recording of financial information in more than one system has a higher priority than SCC that address the above in only one system. The scope is defined as System 1 (S1), System 2 (S2), …, System n (Sn).

3. *Organization's Objectives*–This quality attribute refers to the number of business goals and objectives the SCC satisfies. The higher the number of objectives the SCC satisfies, the higher the priority of the SCC. Organization's objectives are defined with the following features: Objective 1 (O1), Objective 2 (O2), …, Objective n (On).

4. *Physical Access* – SCC will prevent, detect, and/or record unauthorized changes to the organization's physical location access systems (e.g., building facilities, data centers where information processing takes place, the finance/accounting department, human resources department, etc.). The higher the number of physical location access systems addressed by the SCC, the higher the probability of the SCC of being selected. Physical access is defined as Location 1 (L1), Location 2 (L2), …, Location n (Ln).

5. *Access Controls*–Implementation of an SCC for this quality attribute will promote appropriate levels of change management access controls to ensure the protection of the organization's systems/applications against unauthorized

activities. Organizations may implement network access controls (N), operating systems access controls (O), and application controls (A) based on their specific needs.

6. *Human Resources*–Implementation of SCC support reductions of unauthorized access, inadequate change implementations, fraud, or misuse of computer resources by promoting information security awareness (Aw), training (Tn), and education of employees (E). Depending on the particular situation, costs involved, and availability of personnel, organizations may select which of these to employ.

7. *Communications and Operations Management* – SCC will ensure the correct and secure operation of information processing facilities, which includes addressing for adequate segregation of duties (SoD), change management (CM), and network security (NS). Organizations may select SCC to address all of these or just some depending on their particular needs.

8.*Systems Acquisition, Development, and Maintenance* – SCC will support security related to the organization's in-house and/or off-the-shelf systems or applications (e.g., ensure personnel with authorized access can move changes into production environments, etc.). The higher the number of systems or applications addressed by the SCC, the higher the priority of the SCC. Systems Acquisition, Development, and Maintenance are defined as Systems or Applications 1 (SoA1), Systems or Applications 2 (SoA2), …, and Systems or Applications n (SoAn).

9. *Incident Management*–This quality attribute ensures that security-related incidents (e.g., attempts to change/manipulate financial data, etc.) identified within the organization's processing of information are communicated in a timely manner and that corrective action is taken for any exceptions identified. Incident management may apply to online processing and/or batch processing. Incident Management is defined as Processing 1 (P1), Processing 2 (P2), …, and Processing n (Pn).

Using synthetic data for the identified quality attributes and features, an input matrix is generated with synthesized weights for the features of the 10 SCC listed in Table II. Table II corresponds to the input matrix X in Equation (4). The weights represent the weight vector shown in Equation (5) after applying Equations (6) – (8) on each grey number in Table II.

Table III corresponds to the normalized R matrix after applying Equations (9) and (10) on each number in the matrix. Ideal SCC is also shown here corresponding to the vector r0 of Equation (11) after applying Equations (12) and (13) on each column of Table III.

Finally, Table IV shows the Euclidian distance of each SCC implementation from the ideal SCC, as well as the grey relational grade of that implementation and its ranking. The Euclidian distances and grey relational grades are obtained after applying Equations (15) and (16) on each row of Table II.

As Table IV shows, the best SCC to implement is SCC 4 (100%), followed by SCC 2 (99.1%) and SCC 9 (98.4%). It is important to note that the evaluation of SCC using this approach is fully dependent on the particular organization and its security objectives.

Table II. Decision matrix and synthesized weights after feature aggregation.

<table>
<tr><th rowspan="3"></th><th colspan="6">A1</th><th colspan="6">A2</th><th colspan="6">A3</th><th colspan="6">A4</th><th colspan="6">A5</th><th colspan="6">A6</th><th colspan="6">A7</th><th colspan="6">A8</th><th colspan="6">A9</th></tr>
<tr><th colspan="2">C</th><th colspan="2">AoR</th><th colspan="2">T</th><th colspan="2">S1</th><th colspan="2">S2</th><th colspan="2">Sn</th><th colspan="2">O1</th><th colspan="2">O2</th><th colspan="2">On</th><th colspan="2">L1</th><th colspan="2">L2</th><th colspan="2">Ln</th><th colspan="2">N</th><th colspan="2">O</th><th colspan="2">A</th><th colspan="2">Aw</th><th colspan="2">Tn</th><th colspan="2">E</th><th colspan="2">SoD</th><th colspan="2">CM</th><th colspan="2">NS</th><th colspan="2">SoA1</th><th colspan="2">SoA2</th><th colspan="2">SoAn</th><th colspan="2">P1</th><th colspan="2">P2</th><th colspan="2">Pn</th></tr>
<tr><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th></tr>
<tr><td>1</td><td colspan="3">3.66</td><td colspan="3">10.05</td><td colspan="3">3.57</td><td colspan="3">13.69</td><td colspan="3">4.46</td><td colspan="3">11.78</td><td colspan="3">7.50</td><td colspan="3">10.39</td><td colspan="3">4.71</td><td colspan="3">10.15</td><td colspan="3">2.09</td><td colspan="3">7.42</td><td colspan="3">7.87</td><td colspan="3">11.06</td><td colspan="3">2.69</td><td colspan="3">19.10</td><td colspan="3">4.46</td><td colspan="3">9.92</td></tr>
<tr><td>2</td><td colspan="3">4.25</td><td colspan="3">13.41</td><td colspan="3">6.39</td><td colspan="3">10.64</td><td colspan="3">6.95</td><td colspan="3">16.35</td><td colspan="3">5.04</td><td colspan="3">15.23</td><td colspan="3">4.84</td><td colspan="3">7.96</td><td colspan="3">6.20</td><td colspan="3">15.73</td><td colspan="3">5.12</td><td colspan="3">14.44</td><td colspan="3">7.29</td><td colspan="3">11.47</td><td colspan="3">3.24</td><td colspan="3">8.97</td></tr>
<tr><td>3</td><td colspan="3">5.70</td><td colspan="3">13.73</td><td colspan="3">3.94</td><td colspan="3">12.29</td><td colspan="3">2.74</td><td colspan="3">13.93</td><td colspan="3">4.87</td><td colspan="3">9.30</td><td colspan="3">2.42</td><td colspan="3">12.95</td><td colspan="3">5.34</td><td colspan="3">12.54</td><td colspan="3">3.83</td><td colspan="3">14.06</td><td colspan="3">6.24</td><td colspan="3">12.46</td><td colspan="3">5.15</td><td colspan="3">12.61</td></tr>
<tr><td>4</td><td colspan="3">3.17</td><td colspan="3">9.49</td><td colspan="3">6.77</td><td colspan="3">10.60</td><td colspan="3">6.98</td><td colspan="3">15.99</td><td colspan="3">5.38</td><td colspan="3">13.73</td><td colspan="3">6.20</td><td colspan="3">12.54</td><td colspan="3">3.81</td><td colspan="3">16.42</td><td colspan="3">4.46</td><td colspan="3">15.54</td><td colspan="3">1.43</td><td colspan="3">10.60</td><td colspan="3">5.24</td><td colspan="3">13.34</td></tr>
<tr><td>5</td><td colspan="3">5.81</td><td colspan="3">8.81</td><td colspan="3">4.20</td><td colspan="3">11.45</td><td colspan="3">3.87</td><td colspan="3">13.54</td><td colspan="3">5.19</td><td colspan="3">16.46</td><td colspan="3">2.39</td><td colspan="3">11.44</td><td colspan="3">3.84</td><td colspan="3">8.88</td><td colspan="3">8.00</td><td colspan="3">17.36</td><td colspan="3">3.16</td><td colspan="3">16.40</td><td colspan="3">5.00</td><td colspan="3">9.57</td></tr>
<tr><td>6</td><td colspan="3">6.34</td><td colspan="3">13.72</td><td colspan="3">5.45</td><td colspan="3">12.22</td><td colspan="3">3.61</td><td colspan="3">9.74</td><td colspan="3">8.11</td><td colspan="3">16.23</td><td colspan="3">3.39</td><td colspan="3">16.55</td><td colspan="3">4.27</td><td colspan="3">14.23</td><td colspan="3">4.60</td><td colspan="3">12.28</td><td colspan="3">6.20</td><td colspan="3">12.21</td><td colspan="3">2.67</td><td colspan="3">8.30</td></tr>
<tr><td>7</td><td colspan="3">3.52</td><td colspan="3">16.53</td><td colspan="3">2.53</td><td colspan="3">10.50</td><td colspan="3">2.20</td><td colspan="3">11.46</td><td colspan="3">3.48</td><td colspan="3">16.45</td><td colspan="3">3.61</td><td colspan="3">6.81</td><td colspan="3">4.58</td><td colspan="3">11.30</td><td colspan="3">3.03</td><td colspan="3">9.02</td><td colspan="3">3.43</td><td colspan="3">11.39</td><td colspan="3">2.85</td><td colspan="3">12.90</td></tr>
<tr><td>8</td><td colspan="3">4.12</td><td colspan="3">16.44</td><td colspan="3">6.49</td><td colspan="3">12.12</td><td colspan="3">5.98</td><td colspan="3">16.94</td><td colspan="3">3.56</td><td colspan="3">7.91</td><td colspan="3">7.01</td><td colspan="3">13.87</td><td colspan="3">5.67</td><td colspan="3">17.18</td><td colspan="3">3.00</td><td colspan="3">9.31</td><td colspan="3">2.86</td><td colspan="3">12.00</td><td colspan="3">4.35</td><td colspan="3">9.04</td></tr>
<tr><td>9</td><td colspan="3">3.95</td><td colspan="3">10.92</td><td colspan="3">4.80</td><td colspan="3">15.80</td><td colspan="3">2.56</td><td colspan="3">14.56</td><td colspan="3">4.34</td><td colspan="3">10.43</td><td colspan="3">6.06</td><td colspan="3">14.91</td><td colspan="3">5.91</td><td colspan="3">18.49</td><td colspan="3">7.03</td><td colspan="3">15.28</td><td colspan="3">6.97</td><td colspan="3">13.18</td><td colspan="3">2.69</td><td colspan="3">16.23</td></tr>
<tr><td>10</td><td colspan="3">8.59</td><td colspan="3">15.22</td><td colspan="3">5.85</td><td colspan="3">14.01</td><td colspan="3">4.34</td><td colspan="3">12.08</td><td colspan="3">4.48</td><td colspan="3">10.23</td><td colspan="3">7.64</td><td colspan="3">14.24</td><td colspan="3">6.68</td><td colspan="3">13.91</td><td colspan="3">6.60</td><td colspan="3">11.27</td><td colspan="3">7.04</td><td colspan="3">10.95</td><td colspan="3">3.78</td><td colspan="3">8.53</td></tr>
</table>

Wj	0.111	0.039	0.118	0.134	0.136	0.183	0.139	0.073	0.067

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE: 6
JUNE/2019
DOI: 10.33642/ijbass.v5n6p4
https://ijbassnet.com/

Table III. Normalized Matrix and Ideal SCC.

<table>
<tr><th rowspan="3">[redacted]</th><th colspan="6">A1</th><th colspan="6">A2</th><th colspan="6">A3</th><th colspan="6">A4</th><th colspan="6">A5</th><th colspan="6">A6</th><th colspan="6">A7</th><th colspan="6">A8</th><th colspan="6">A9</th></tr>
<tr><th colspan="2">C</th><th colspan="2">AoR</th><th colspan="2">T</th><th colspan="2">S1</th><th colspan="2">S2</th><th colspan="2">Sn</th><th colspan="2">O1</th><th colspan="2">O2</th><th colspan="2">On</th><th colspan="2">L1</th><th colspan="2">L2</th><th colspan="2">Ln</th><th colspan="2">N</th><th colspan="2">O</th><th colspan="2">A</th><th colspan="2">Aw</th><th colspan="2">Tn</th><th colspan="2">E</th><th colspan="2">SoD</th><th colspan="2">CM</th><th colspan="2">NS</th><th colspan="2">SoA1</th><th colspan="2">SoA2</th><th colspan="2">SoAn</th><th colspan="2">P1</th><th colspan="2">P2</th><th colspan="2">Pn</th></tr>
<tr><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th><th colspan="3">l</th><th colspan="3">u</th></tr>
<tr><td>1</td><td colspan="3">0.005</td><td colspan="3">0.013</td><td colspan="3">0.002</td><td colspan="3">0.006</td><td colspan="3">0.006</td><td colspan="3">0.016</td><td colspan="3">0.011</td><td colspan="3">0.253</td><td colspan="3">0.008</td><td colspan="3">0.016</td><td colspan="3">0.004</td><td colspan="3">0.263</td><td colspan="3">0.017</td><td colspan="3">0.017</td><td colspan="3">0.002</td><td colspan="3">0.016</td><td colspan="3">0.004</td><td colspan="3">0.009</td></tr>
<tr><td>2</td><td colspan="3">0.005</td><td colspan="3">0.017</td><td colspan="3">0.003</td><td colspan="3">0.005</td><td colspan="3">0.009</td><td colspan="3">0.022</td><td colspan="3">0.008</td><td colspan="3">0.308</td><td colspan="3">0.008</td><td colspan="3">0.013</td><td colspan="3">0.012</td><td colspan="3">0.353</td><td colspan="3">0.022</td><td colspan="3">0.022</td><td colspan="3">0.006</td><td colspan="3">0.009</td><td colspan="3">0.003</td><td colspan="3">0.008</td></tr>
<tr><td>3</td><td colspan="3">0.007</td><td colspan="3">0.017</td><td colspan="3">0.002</td><td colspan="3">0.006</td><td colspan="3">0.004</td><td colspan="3">0.018</td><td colspan="3">0.007</td><td colspan="3">0.240</td><td colspan="3">0.004</td><td colspan="3">0.021</td><td colspan="3">0.011</td><td colspan="3">0.319</td><td colspan="3">0.021</td><td colspan="3">0.021</td><td colspan="3">0.005</td><td colspan="3">0.010</td><td colspan="3">0.005</td><td colspan="3">0.011</td></tr>
<tr><td>4</td><td colspan="3">0.004</td><td colspan="3">0.012</td><td colspan="3">0.003</td><td colspan="3">0.005</td><td colspan="3">0.009</td><td colspan="3">0.021</td><td colspan="3">0.008</td><td colspan="3">0.291</td><td colspan="3">0.010</td><td colspan="3">0.020</td><td colspan="3">0.008</td><td colspan="3">0.361</td><td colspan="3">0.024</td><td colspan="3">0.024</td><td colspan="3">0.001</td><td colspan="3">0.009</td><td colspan="3">0.005</td><td colspan="3">0.012</td></tr>
<tr><td>5</td><td colspan="3">0.007</td><td colspan="3">0.011</td><td colspan="3">0.002</td><td colspan="3">0.005</td><td colspan="3">0.005</td><td colspan="3">0.018</td><td colspan="3">0.008</td><td colspan="3">0.322</td><td colspan="3">0.004</td><td colspan="3">0.018</td><td colspan="3">0.008</td><td colspan="3">0.279</td><td colspan="3">0.026</td><td colspan="3">0.026</td><td colspan="3">0.003</td><td colspan="3">0.013</td><td colspan="3">0.004</td><td colspan="3">0.009</td></tr>
<tr><td>6</td><td colspan="3">0.008</td><td colspan="3">0.017</td><td colspan="3">0.002</td><td colspan="3">0.005</td><td colspan="3">0.005</td><td colspan="3">0.013</td><td colspan="3">0.012</td><td colspan="3">0.319</td><td colspan="3">0.005</td><td colspan="3">0.027</td><td colspan="3">0.008</td><td colspan="3">0.337</td><td colspan="3">0.019</td><td colspan="3">0.019</td><td colspan="3">0.005</td><td colspan="3">0.010</td><td colspan="3">0.002</td><td colspan="3">0.007</td></tr>
<tr><td>7</td><td colspan="3">0.004</td><td colspan="3">0.021</td><td colspan="3">0.001</td><td colspan="3">0.005</td><td colspan="3">0.003</td><td colspan="3">0.015</td><td colspan="3">0.005</td><td colspan="3">0.322</td><td colspan="3">0.006</td><td colspan="3">0.011</td><td colspan="3">0.009</td><td colspan="3">0.305</td><td colspan="3">0.014</td><td colspan="3">0.014</td><td colspan="3">0.003</td><td colspan="3">0.009</td><td colspan="3">0.003</td><td colspan="3">0.012</td></tr>
<tr><td>8</td><td colspan="3">0.005</td><td colspan="3">0.021</td><td colspan="3">0.003</td><td colspan="3">0.005</td><td colspan="3">0.008</td><td colspan="3">0.022</td><td colspan="3">0.005</td><td colspan="3">0.224</td><td colspan="3">0.011</td><td colspan="3">0.022</td><td colspan="3">0.011</td><td colspan="3">0.369</td><td colspan="3">0.014</td><td colspan="3">0.014</td><td colspan="3">0.002</td><td colspan="3">0.010</td><td colspan="3">0.004</td><td colspan="3">0.008</td></tr>
<tr><td>9</td><td colspan="3">0.005</td><td colspan="3">0.014</td><td colspan="3">0.002</td><td colspan="3">0.007</td><td colspan="3">0.003</td><td colspan="3">0.019</td><td colspan="3">0.007</td><td colspan="3">0.253</td><td colspan="3">0.010</td><td colspan="3">0.024</td><td colspan="3">0.012</td><td colspan="3">0.383</td><td colspan="3">0.023</td><td colspan="3">0.023</td><td colspan="3">0.006</td><td colspan="3">0.011</td><td colspan="3">0.002</td><td colspan="3">0.015</td></tr>
<tr><td>10</td><td colspan="3">0.011</td><td colspan="3">0.019</td><td colspan="3">0.003</td><td colspan="3">0.006</td><td colspan="3">0.006</td><td colspan="3">0.016</td><td colspan="3">0.007</td><td colspan="3">0.251</td><td colspan="3">0.012</td><td colspan="3">0.023</td><td colspan="3">0.013</td><td colspan="3">0.334</td><td colspan="3">0.017</td><td colspan="3">0.017</td><td colspan="3">0.006</td><td colspan="3">0.009</td><td colspan="3">0.003</td><td colspan="3">0.008</td></tr>
</table>

Table IV. Euclidian distances, relational grades, and rankings of all SCC.

[redacted]	Pj	Rj	Qj	Uj
1	0.324	0.009	0.338	0.806
2	0.405	0.011	0.416	0.991
3	0.352	0.012	0.362	0.863
4	0.405	0.008	0.420	1.000
5	0.375	0.009	0.376	0.897
6	0.399	0.013	0.408	0.972
7	0.368	0.013	0.377	0.900
8	0.367	0.013	0.376	0.897
9	0.400	0.009	0.413	0.984
10	0.365	0.015	0.373	0.889

5. Contributions and Future Research

There are several important contributions to this research. First, the methodology is simple, can be easily implemented in a spreadsheet or software tool, and promote usage in practical scenarios where highly complex methodologies for SCC selection are impractical. Second, the methodology fuses multiple-attribute assessment criteria and features to provide a holistic view of the overall SCC quality. Third, the methodology is easily extended to include additional attributes and features not considered within this research. This is possibly the most meaningful contributions from this research. Finally, the methodology provides a mechanism to evaluate the quality of SCC in various domains. Overall, the methodology developed and presented in this research proved to be a feasible technique for assessing SCC in organizations.

Opportunities for future work exist that can enhance the proposed solution to improve the overall quality of the SCC selection process. For instance, traditional methodologies nor our proposed solution herein consider the true degree of relevance (imprecise in nature) when evaluating SCC. The above still represents a major problem for organizations that can potentially impact the overall security over the information.

An assessment methodology that accounts for organizations' goals while adequately modeling imprecise parameters can guarantee an effective selection of SCC. Fuzzy Set Theory (FST), for instance, allows for a more accurate assessment of imprecise parameters than traditional methodologies. When using FST, propositions can be true to some degree, allowing for logical reasoning with partially true imprecise statements (Das, 2009). In other words, truth values are no longer restricted to the two values 'true' and 'false', but expressed by the linguistic variables 'true' and 'false' (Zimmermann, 2010). An evaluation of SCC using FST will lead to a thorough, more detailed assessment (Otero & Otero, 2011; Ejnioui, Otero & Qureshi, 2012), thus, supporting a more effective SCC evaluation. Moreover, based on the literature reviewed, there has not been a research study that specifically evaluated and prioritized SCC in organizations using FST.

While grey numbers can handle easily ambiguous and imprecise data, grey systems still do not provide powerful analytical tools available in fuzzy sets. Since the latter has been around for more time, a number of analysis and optimization techniques have been developed to tackle challenging problems with imprecise data such as the ones described above. However, the power and sophistication of these fuzzy techniques impose sometimes a computational burden and a conceptual complexity that may defeat the initial purpose of simple and practical approaches needed to assess SCC.

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

EISSN: 2469-6501
VOL: 5, ISSUE: 6
JUNE/2019
DOI: 10.33642/ijbass.v5n6p4
https://ijbassnet.com/

phenomena (Zimmermann, 2010). Additionally, FST has been used as modeling, problem-solving, and data mining tool, and has proven superior to existing methods as well as attractive to enhance classical approaches.

A further potential research opportunity would involve examining results from this research as well as from other similar SCC assessment methodologies with the purpose of comparing them to determine which method is the most effective.

6. Conclusions

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 a review of the literature, a key limitation identified of current SCC assessment methodologies is that imprecise parameters are being modelled as precise ones. To address this limitation, a GST-based SCC assessment methodology was proposed. The proposed methodology assists 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 also assures organizations that only the best and most appropriate SCC will get implemented while maintaining a well-designed and controlled information system environment.

The research presented in this paper develops an innovative approach for evaluating the quality of SCC in organizations based on multiple-attribute assessment criteria. Specifically, it presents a methodology that uses GST to create a unified measurement that represents how well SCC meet quality attributes and their related features. Through a case study, the approach is proven successful in providing a way for measuring the quality of SCC consistent with organizational goals and objectives.

References

Backhouse, J., and Dhillon, G. (1996). Structures of responsibility and security of information systems. European Journal of Information Systems, 5, 2–9. doi:10.1057/ejis.1996.7.

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

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. ACM Computing Surveys, 25, 375–414. doi:10.1145/162124.162127.

Baskerville, R., and Siponen, M. (2002). An information security meta-policy for emergent organizations, Journal of Logistics Information Management, 15, 337-346.

Chang, W. C. (2000). A comprehensive study of grey relational generating. *Journal of Grey System*, *3*(3), 53–63.

Chen, Z., & Yoon, J. (2010). IT auditing to assure a secure cloud computing. In *Proceedings of the 6th World Congress on Services* (pp. 253-259).

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

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

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).

Dhillon, G., and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16, 293–314.

Ejnioui, A., Otero, C. E., & Qureshi, A. (2012). Software requirement prioritization using fuzzy multi-attribute decision making. *IEEE Conference on Open Systems*, 1-6.

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

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

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).

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).

Herath, T., and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness, Decision Support Systems, 47, 154-165.

Hornstein, H. A. (2015). The integration of project management and organizational change management is now a necessity, *International Journal of Project Management*, *33*(2), 291-298.

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).

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).

Information Technology Infrastructure Library (ITIL) Change Management. (2016). BMC Software, Inc., www.bmc.com/guides/itil-change-management.html

Jee, D. H., and Kang, K. J. (2000). A method for optimal material selection aided with decision making theory. Materials & Design, 21, 199–206. doi:10.1016/ S0261-3069(99)00066-7.

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

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).

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

Krishnan, G. V., and 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, 73-90.

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).

Lin, Y.-H., Lee, P.-C., and Chang, T.-P. (2008). Integrating grey number and Minkowski distance function into grey relational analysis technique to improve the decision quality under uncertain information. Construction Management and Economics, 26, 115–123. doi:10.1080/01446190701821802.

Liu, S., & Lin, Y. (2011). *Grey systems: Theory and applications*. Berlin Heiderlberg, Germany: Springer-Verlag.

Masli, A., Richardson, V.J., Watson, M.W., and Zmud, R.W. (2016). Senior Executives' IT Management Responsibilities: Serious IT-Related Deficiencies and CEO/CFO Turnover, MIS Quarterly, 40, 687-708.

Mitra, P., and Mishra, S. (2016). Behavioral aspects of ERP implementation: A conceptual review, Interdisciplinary Journal of Information, Knowledge, and Management, 11, 17-30.

Morgan, S. (2017, October 16). Cybercrime Damages $6 Trillion By 2021. Retrieved May 20, 2019, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

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).

Otero, A. R. (2015). 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 Edition*. Boca Raton, FL. CRC Press and Auerbach Publications.

Otero, A. R., Ejnioui, A., Otero, C. E., and Tejay, G. (2011). Evaluation of Information Security Controls in Organizations by Grey Relational Analysis, International Journal of Dependable and Trustworthy Information Systems, 2, 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., Otero, C. E., and Qureshi, A. (2010). A multi-criteria evaluation of information security controls using Boolean features. International Journal of Network Security & Its Applications, 2, 1–11. doi:10.5121/ijnsa.2010.2401.

Otero, L. D., and Otero, C. E. (2011). A fuzzy expert system architecture for capability assessments in skill-based environments, Expert Systems with Applications, 39, 654-662.

Pillai, A. K. R., Pundir, A. K., and Ganapathy, L. (2014). Improving Information Technology Infrastructure Library Service Delivery Using an Integrated Lean Six Sigma Framework: A Case Study in a Software Application Support Scenario, Journal of Software Engineering and Applications, 1, 483-497. http://dx.doi.org/10.4236/jsea.2014.76045

Rao, R. V., and Patel, B. K. (2010). A subjective and objective integrated multiple attribute decision making method for material selection. Materials & Design, 31, 4738–4747. doi:10.1016/j.matdes.2010.05.014.

Rui, X., and Wunshch, D. C. (2005). Survey of clustering algorithms. IEEE Transactions on Neural Networks, 16, 645–678. doi:10.1109/ TNN.2005.845141 PMID:15940994.

Ryan, V. (2019, May 13). CCH Tax Software Outage Leaves Accountants in Limbo. Retrieved May 17, 2019, from http://www.cfo.com/tax/2019/05/cch-software-outage-leaves-accountants-in-limbo/

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

Schwartz, M. (1990). Computer security: Planning to protect corporate assets, Journal of Business Strategy, 11, 38-41.

EISSN: 2469-6501
VOL: 5, ISSUE: 6
JUNE/2019
DOI: 10.33642/ijbass.v5n6p4
https://ijbassnet.com/

Shanian, A., and Savadogo, O. (2006). TOPSIS multiple-criteria decision support analysis for material selection of metallic bipolar plates for polymer electrolyte fuel cell. Journal of Power Sources, 159, 1095–1104. doi:10.1016/j.jpowsour.2005.12.092.

Singh, A.N., Picot, A., Kranz, J., Gupta, M.P., and Ojha, A. (2013). Information security management (ISM) practices: lessons from select cases from India and Germany, Global Journal of Flexible Systems Management, 14, 225-239.

Thomé, J., Shar, L. K., Bianculli, D., and Briand, L. (2018). Security slicing for auditing common injection vulnerabilities, Journal of Systems and Software, 137, 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., and Von Solms, R. (2003). A model for deriving information security controls attribute profiles, Computers & Security, 22, 233-244.

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

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.

Yamaguchi, D., Li, G. D., Mizutani, K., Akabane, T., Nagai, M., and Kitaoka, M. (2006). On the generalization of grey relational analysis. Journal of Grey System, 9, 23–34.

Yamaguchi, D., Li, G. D., and Nagai, M. (2005). New grey relational analysis for finding the invariable structure and its applications. Journal of Grey System, 8, 167–178.

Yoon, K. P., and Hwang, C. L. (1985). Manufacturing plant location analysis by multiple attribute decision making: Part I–Single-plant strategy. International Journal of Production Research, 23, 345–359. doi:10.1080/00207548508904712.

Zhang, J., Wu, D., and Oslon, D. L. (2005). The method of grey relational analysis to multiple attribute decision making problems with interval numbers. Mathematical and Computer Modelling, 1–8.

Zimmermann, H. -J. (2010). *Fuzzy Set Theory*. New York, NY: John Wiley & Sons, Inc.