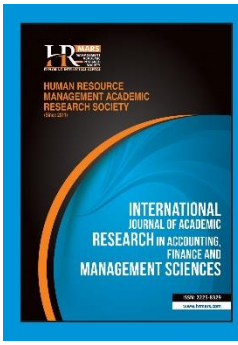


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL

www.hrmars.com
ISSN: 2225-8329

Accounting Environment: Ranking of Internal Controls to Safeguard Accounting Information and its Integration with IT Operations

Angel R. Otero

To Link this Article: http://dx.doi.org/10.6007/IJARAFMS/v11-i3/10874 DOI:10.6007/IJARAFMS /v11-i3/10874

Received: *21* June 2021*,* ***Revised:*** *23* July 2021*,* ***Accepted:*** *09* August 2021

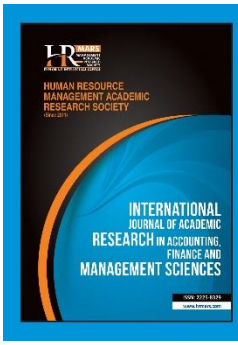
Published Online: 26 August 2021

In-Text Citation: (Otero, 2021)

To Cite this Article: Otero, A. R. (2021). Accounting Environment: Ranking of Internal Controls to Safeguard Accounting Information and its Integration with IT Operations. *International Journal of Academic Research in Accounting Finance and Management Sciences*, *11*(3), 283–302.

Vol. 11, No. 3, 2021, Pg. 283 - 302

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


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY
EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2225-8329

Accounting Environment: Ranking of Internal Controls to Safeguard Accounting Information and its Integration with IT Operations

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

Abstract
Cyber criminals continue targeting organizations' accounting information mostly because of its sensitivity and high value. This leads to devastating losses that impact the confidentiality, integrity, and availability of such information. General Information Technology Controls related to computer operations or GITC-CO are critical in ensuring the security, integrity, completeness, and reliability of accounting information. Per the literature reviewed, traditional methodologies do not necessarily promote an effective assessment of these types of controls in organizations, preventing the implementation of required controls and/or the exclusion of unnecessary controls. The aim of this research is to develop an assessment methodology, based on Grey Systems Theory, that will adequately address weaknesses identified in traditional assessment methodologies, resulting in a more accurate selection of controls. Through a case evaluation, the approach proved successful in providing a more precise and complete evaluation of GITC-CO in organizations.
Keywords: Internal Controls, General IT Controls, Accounting, Grey Systems Theory

Introduction

Cyber criminals continue targeting organizations' accounting information mostly because of its high value. In fact, by the year 2021, the cybercrime's global cost is estimated to reach $6 trillion (Cybercrime Damages, 2016; Otero & Fink, 2020). Such constant attacks lead to devastating losses resulting in the loss of confidentiality, integrity, and availability of sensitive accounting information (Kuhn & Morris, 2017; Ponemon, 2016). Examples of sensitive accounting information constantly attacked, based on Tucker (2018), include transactions associated with globalization, intercompany trades, and mergers and acquisitions as these transactions create major risks related to financial and regulatory reporting. A 2016 survey conducted by the Sarbanes-Oxley Act of 2002 (SOX) & Internal Controls Professionals Group suggested that increasing the focus on cyber and information technology (IT) controls around accounting software systems was top priority for organizations to protect their information (SOX & Internal Controls Professionals Group, 2017). Figure 1 shows primary attack points for

data breaches in the U.S. as of 2018, evidencing software as the primary attack point (Centrify, 2019).

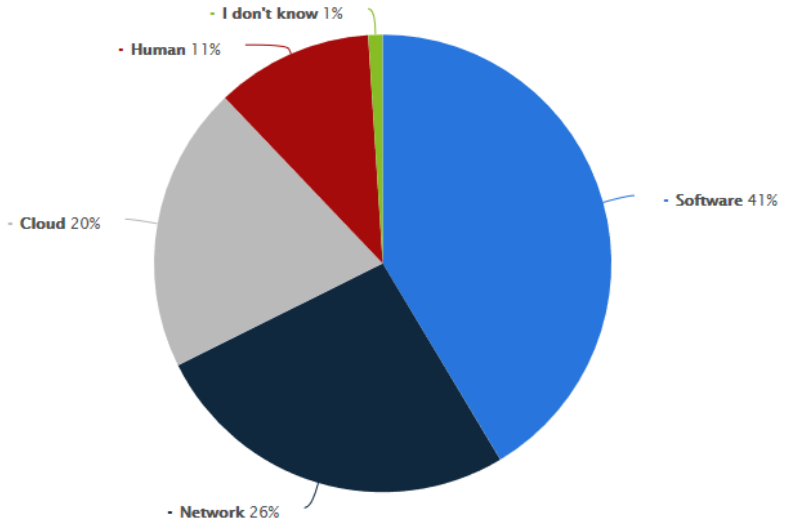


Figure 1: Primary attack points for data breaches in the U.S. as of 2018

Organizations must implement adequate controls to safeguard their software systems hosting accounting information. According to Lavion (2018); Otero (2014), the absence of controls or the implementation of weak controls open up opportunities for attacks, such as the above, or fraud to take place. Corporate fraud, based on FBI (2019), is among the Federal Bureau of Investigation's (FBI) highest criminal priorities. Corporate fraud translates into significant losses for companies and their investors and continues to cause immeasurable damage to the U.S. economy. The majority of the corporate fraud identified by the FBI involves accounting information in the form of fraudulent trades; false accounting entries; data manipulation; misrepresentations of financial condition; and/or illicit transactions to evade regulatory oversight (FBI, 2019).

Web applications are also susceptible to many security risks and vulnerabilities dealing with accounting information, thus creating significant exposure for many organizations (ISACA, 2011; Thomé, Shar, Bianculli, & Briand, 2018). Based on a 2017 study by the American Accounting Association, organizations with weak entity-level controls were 90% or more prone to have fraud versus organizations with established strong controls (Donelson, Ege, & McInnis, 2017). The need for implementing strong controls is forcing organizations to invest more time revaluating risks and identifying controls that are effective and efficient to ensure prevention of fraud and safeguarding of information (Otero, 2019a; Kuhn, Ahuja, & Mueller, 2013).

Organizations must design and implement internal controls that can protect the information, mitigate risks preventing a company from achieving its business objectives, and remain in compliance with existing laws and regulations (Lavion, 2018; Deloitte, 2018; GTAG 8, 2009; Otero, Tejay, Otero, & Ruiz, 2012). Business objectives, such as, reliability of the entity's financial reporting process, effectiveness and efficiency of operations, and compliance with applicable laws and regulations are common objectives constantly threatened in an organization (Otero, 2018; Otero, Ejnioui, Otero, & Tejay, 2011).

Internal controls related to IT or General IT Controls (GITC) support the effective functioning of applications, the integrity of reports generated from those applications, and

the security of data housed within the applications (Kuhn & Morris, 2017; Otero, 2019b). GITC commonly include controls over (1) computer or information systems operations; (2) access security; and (3) change management. GITC over computer operations (GITC-CO) must be in place to ensure the security, integrity, completeness, and reliability of accounting information (Keef, 2019; GTAG 2, 2012; Otero, 2015a). They provide a structure for the day-to-day management of operations and maintenance of existing systems. GITC-CO typically assessed by organizations relate to: operating policies and procedures; data processing; protection of data files and programs; physical security and access controls; environmental controls; program and data backups; and continuity plans (Otero, Sonnenberg & Bean, 2019).

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

The aim of this research is to develop an assessment methodology, based on Grey Systems Theory (GST), that will adequately address weaknesses identified in traditional GITC-CO assessment methodologies, resulting in a more accurate selection of GITC-CO. It is argued that a GST-based assessment methodology will consider imprecise parameters (in the form of organizations' criteria) when evaluating GITC-CO and, most importantly, quantify and rank such parameters using real numbers. The remainder of this research paper is organized as follows. Section 2 provides a summary of the literature reviewed related to GITC-CO evaluation and selection. Section 3 explains the theory to be used in the development of the proposed methodology. Section 4 presents the results of a GITC-CO case evaluation/optimization using the proposed approach, while Section 5 and 6 present discussions and conclusions, respectively.

Literature Review

According to Barnard and Von Solms (2000), the process of identifying effective GITC-CO in organizations has been a challenge in the past. For instance, risk analysis and management (RAM) has been recognized in the literature as an effective approach to identify GITC-CO (Barnard & Von Solms, 2000). RAM consists of performing business analyses to determine information security requirements (Barnard & Von Solms, 2000). GITC-CO are then put into place to mitigate the risks resulting from the analyses performed. RAM, however, has been described as a subjective, bottom-up approach (Van der Haar & Von Solms, 2003), not necessarily taking into account unique organizational constraints.

The use of 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 GITC-CO. Some best practices include: Control Objectives for Information and related Technology (COBIT); Information Technology Infrastructure Library (ITIL); the National Institute of Standards and Technology (NIST); and the 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 GITC-CO, such as, International Standardization Organization (ISO) / International Electrotechnical Commission (IEC) 27001 and 27002 and the Capability Maturity Model (CMM).

Selecting effective GITC-CO from best practice frameworks can be challenging. 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).

In a different study, a model was developed for defining and recommending legal requirements and relevant controls (Gerber & Von Solms, 2008). Legal information security requirements resulted from a legal compliance questionnaire combined with a matrix that mapped 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 GITC-CO, was produced to satisfy the previously identified legal requirements. Nonetheless, as evidenced earlier, selection of controls from best practice frameworks like ISO/IEC 27002 offers minimum guidance in determining effective controls for a particular organization (Van der Haar & Von Solms, 2003).

In Otero, Otero, and Qureshi (2010), an innovative control evaluation and selection approach was developed, particularly for information security GITC-CO 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 control after taking into account benefits and restrictions associated with implementing the particular control (Otero, Sonnenberg & Delgado-Perez, 2020). Through a case study, the approach proved successful in providing a way for measuring the quality of information security GITC-CO in organizations. However, the boolean criteria the authors used for evaluating the quality attributes of controls to ultimately determine which ones to select, may not be considered a precise enough assessment for selecting and ultimately implementing controls in organizations.

Another common method used to select GITC-CO in organizations is through checklists. Chen and Yoon (2010) used checklists as a framework to identify common GITC-CO, including information security risks, within cloud-based organizations. 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). However, 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). 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.

In Otero (2015b), a methodology was developed using fuzzy set theory to address weaknesses in the existing literature pertaining to the evaluation of GITC-CO in organizations' financial systems. The methodology resulted in a more effective selection and enhanced information security in organizations (Otero, 2015b; Otero, 2020; Otero, Tejay, Otero, & Ruiz, 2012). Due to convenience and availability, the research performed by Otero (2015b) involved

a single university located in the southeast U.S. within the schools, universities, and non-profit industry. However, further similar studies must be performed at organizations in other locations, or from different sizes and industry types in order to generalize the findings in a broader scope. Also, implementation of the design-science research (DSR) method used to develop the methodology, represents a limitation given the rapid advances in technology that can potentially upset its results before they are implemented successfully in organizations (Hevner, March, Park, & Ram, 2004).

In Rahimian, Bajaj, and Bradley (2016), an Operational, Public image, Legal (OPL) method was proposed, using DSR, to classify the security criticality of the organization's data along three dimensions (i.e., operations, public image, and firm's compliance). Through empirical study, the authors demonstrated how the OPL method allowed for a quantitative estimation of the significance of existing GITC-CO, as well as the risk of missing controls. Questionnaires were completed by senior information security officers and internal auditors supporting the developed model, and its acceptability and usefulness in the organization. Nonetheless, the significance of information security checklists or questionnaires has declined simply "because they provide little by way of analytical stability" (p. 294). Moreover, Backhouse and Dhillon (1996) argued that although checklists or questionnaires draw concern on particular details of procedures, they do not completely address the key task of understanding the substantive questions.

Another research study from Al-Safwani, Fazea, and Ibrahim (2018) developed a GITC computer information security prioritization model to determine critical controls consistent with an assessment criterion. The model used techniques from the Order Performance by Similarity to Ideal Solution (TOPSIS) method (a sub-method of multiple attribute decision making). Assessment of controls with TOPSIS involved a multi- and dynamic evaluation model that assists organizations in evaluating controls accurately. The model enabled adequate security decision making by considering assigned weights of each assessment criterion within the organization. With management-assigned weights, TOPSIS helped the organization implement only the most effective and critical controls. Nevertheless, significant decision making based strictly on management's assigned weights (subjective in nature) may not necessarily be the most objective, nor considered a precise enough assessment for selecting controls in organizations.

Bettaieb, Shin, Sabetzadeh, Briand, Nou, and Garceau (2019) developed an automated decision support system to assist in the identification of GITC for a banking domain. The developed system was based on machine learning and leveraged historical data from security assessments performed over past banking systems. Results suggested that the system provided effective decision support for controls. However, evaluation metrics were limited in scope to GITC controls for which there were at least five occurrences in the historical data. Generalizability of results represented another limitation and important concern of the research. Additional studies (including more longitudinal studies) are needed for validating whether the developed system remains effective in other application contexts, and to ensure the accuracy and relevance of the automated selection process. Based on the reviewed literature, we are not aware of any other studies that have addressed the evaluation of GITC-CO in organizations.

Theoretical Basis

Grey Systems Theory

Grey Systems Theory (GST) has significantly contributed in the areas of grey algebraic systems, equations, and matrices; 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 (Liu & Lin, 2011; Ejnioui, Otero, Tejay, Otero, & Qureshi, 2012). 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 $\otimes$ 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 $\otimes x = \left[\underline{x}, \overline{x}\right] = \left\{x | \underline{x} \leq x \leq \overline{x}, \underline{x} \in \mathbb{R} \text{ and } \overline{x} \in \mathbb{R}\right\}$. 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 $\underline{x} \to -\infty \text{ and } \overline{x} \to \infty$, 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 $\otimes x = \left[\underline{x}, \overline{x}\right]$, 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 $k \times \otimes x = k \times \left[\underline{x}, \overline{x}\right] = \left[k\underline{x}, k\overline{x}\right]$ 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):

$$L_p(\otimes x, \otimes y) = \frac{1}{\sqrt[p]{2}} \sqrt[p]{\left(|\overline{x} - \overline{y}|^p + |\underline{x} - \underline{y}|^p\right)}, p > 0 \qquad (3.1)$$

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

$$L_p(\otimes x, \otimes y) = \frac{1}{\sqrt[p]{2}} \sqrt[p]{\sum_{j=1}^{m} w_j \left(|\overline{x}_j - \overline{y}_j|^p + |\underline{x}_j - \underline{y}_j|^p\right)} \qquad (3.2)$$

where w_j is the weight of the *j*th attribute.

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 GITC-CO in organizations. In the past, this

information uncertainty has been modelled using fuzzy sets (Klir & Yuan, 1995) or grey numbers (Liu & Lin, 2011). While the former has been around for some time, the interest in the latter has increased recently since uncertainty can be modelled and manipulated in more flexible ways than fuzzy sets.

Selection of GITC-CO

The first step involves identifying a set of GITC-CO that could be implemented in the organization. These GITC-CO can be obtained from best practice frameworks listed in Section 2. For instance, ITIL, COBIT, and ISO/IEC 27001 and 27002, all offer best practices or controls to help organizations ensure that all computer operations are appropriately managed. Once selected, the GITC-CO are captured in the GITC-CO vector I as:

$$I = \begin{bmatrix} I_1 \\ I_2 \\ \vdots \\ I_n \end{bmatrix} \qquad (3.3)$$

Attributes and Features

When planning to implement GITC-CO, it is often necessary to address attributes and features important in the decision problem. Each GITC-CO 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, GITC-CO can be evaluated based on the *Scope* attribute. In other words, GITC-CO 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 GITC-CO 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 GITC-CO based on *Scope* would be one where *System* 1, *System* 2, and *System n* have higher evaluation values. Similarly, the least important GITC-CO based on the *Scope* is one where *System* 1, *System* 2, and *System n* have lower evaluation values. As a result, the overall assessment of the *n* GITC-CO based on all *m* features of all quality attributes is captured using the following decision matrix *X*:

$$X = \begin{bmatrix} [\underline{x}_{11}, \overline{x}_{11}] & [\underline{x}_{12}, \overline{x}_{12}] & \dots & [\underline{x}_{1m}, \overline{x}_{1m}] \\ [\underline{x}_{21}, \overline{x}_{21}] & [\underline{x}_{22}, \overline{x}_{22}] & \dots & [\underline{x}_{2m}, \overline{x}_{2m}] \\ \vdots & \vdots & & \vdots \\ [\underline{x}_{n1}, \overline{x}_{n1}] & [\underline{x}_{n2}, \overline{x}_{n2}] & \dots & [\underline{x}_{nm}, \overline{x}_{nm}] \end{bmatrix} \qquad (3.4)$$

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

Feature Weights

In general, a GITC-CO 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 GITC-CO 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:

$$W = [w_1\ w_2\ \cdots\ w_m] \qquad (3.5)$$

where w_j represents the importance of feature f_j. 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), statistical variance is effective and easy to implement (Rao & Patel, 2010). Unlike statistical analysis where 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 $\otimes x = \left[\underline{x}, \overline{x}\right]$ be a grey number with $\underline{x} < \overline{x}$. If $\otimes x$ is continuous, then,

$$\hat{x} = \frac{1}{2}\left(\underline{x} + \overline{x}\right) \qquad (3.6)$$

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:

$$v_j = \frac{1}{n}\sum_{i=1}^{n}\left(\hat{x}_{ij} - \overline{x}_j\right)^2 \qquad (3.7)$$

where $\hat{x}_{ij}$ is the core of grey number $\otimes x_{ij}$ while $\overline{x}_j$ 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:

$$w_j = \frac{v_j}{\sum_{k=1}^{m} v_k} \qquad (3.8)$$

for *j* = 1, 2, …, *m*.

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):

$$\otimes r_{ij} = \frac{\otimes x_{ij}}{\max\limits_{1\le i\le n} \overline{x}_{ij}} = \left[\frac{\underline{x}}{\max\limits_{1\le i\le n} \overline{x}_{ij}}, \frac{\overline{x}}{\max\limits_{1\le i\le n} \overline{x}_{ij}}\right] \qquad (3.9)$$

$$\otimes r_{ij} = -\frac{\otimes x_{ij}}{\min\limits_{1\le i\le n} \underline{x}_{ij}} + 2 = \left[\frac{-\underline{x}}{\min\limits_{1\le i\le n} \underline{x}_{ij}} + 2, \frac{-\overline{x}}{\min\limits_{1\le i\le n} \underline{x}_{ij}} + 2\right] \quad (3.10)$$

where equation (3.9) is applied to maximization features while equation (3.10) is applied to minimization features. The obtained matrix will be the normalized matrix *R*.

The Ideal GITC-CO Implementation

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

$$r_0 = [r_{01}, r_{02}, \dots, r_{0m}] \quad (3.11)$$

where

$$r_{0j} = \max_{1\le i\le n} \overline{r}_{ij}, j \in \{1, 2, \dots, k\} \quad (3.12)$$

and

$$r_{0j} = \min_{1\le i\le n} \underline{r}_{ij}, j \in \{k+1, k+2, \dots, m\} \quad (3.13)$$

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 GITC-CO alternative in *R* can be higher in some features while lower in others. As a result, a compromise GITC-CO implementation must be found in *R* that is as close as possible to the ideal implementation.

Distance Between the Ideal GITC-CO and the GITC-CO Implementations

Equation (3.2) can be used to compute the Minkowski distance between the ideal GITC-CO and each GITC-CO implementation in the *R* matrix as follows:

$$L_p(r_0, \otimes r_i) = \frac{1}{\sqrt[p]{2}} \sqrt[p]{\sum_{j=1}^{m} w_j \left(|r_{0j} - \overline{r}_{ij}|^p + |r_{0j} - \underline{r}_{ij}|^p\right)} \quad (3.14)$$

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 (3.14) to the Euclidian distance in equation (3.15) (Lin et al., 2008; Yoon & Hwang, 1985):

$$L_2(r_0, \otimes r_i) = \frac{1}{\sqrt{2}} \sqrt{\sum_{j=1}^{m} w_j \left(\left(r_{0j} - \overline{r}_{ij}\right)^2 + \left(r_{0j} - \underline{r}_{ij}\right)^2\right)} \quad (3.15)$$

Grey Relational Grade

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

$$g_i = \frac{\max\limits_{1\le i\le n}\left(L_2(r_0, \otimes r_i)\right) - L_2(r_0, \otimes r_i)}{\max\limits_{1\le i\le n}\left(L_2(r_0, \otimes r_i)\right) - \min\limits_{1\le i\le n}\left(L_2(r_0, \otimes r_i)\right)} \qquad (3.16)$$

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

Case Evaluation

This section presents the results of a GITC-CO case evaluation using the proposed assessment methodology applied in the context of a fictitious organization implementing ISO/IEC 27002, an international cybersecurity management standard. The organizational requirement is to determine the most effective controls in order to mitigate risks to accounting information. For evaluation purposes, we focused on quality attributes defined within the ISO/IEC 17799 and 27002 (Da Veiga & Eloff, 2007; Nachin, Tangmanee, & Piromsopa, 2019; ISACA, 2009). We generated synthetic (simulated) data for cybersecurity quality attributes and features for the input matrix. The synthetic data represents real-life operational data from an organization's cybersecurity program. Overall, the case evaluates 10 GITC-CO based on the quality attributes described in next sub-section.

Cybersecurity Quality Attributes

This section presents nine quality attributes defined within ISO/IEC 17799 and 27002.

Restrictions. There are restrictions that management must take into account before selecting and implementing GITC-CO. These may include whether the costs involved in the selection and implementation of the GITC-CO are high, whether resources are not available, and whether there are scheduling constraints associated with implementing the particular GITC-CO. The presence of any of the above will negatively affect the specific quality attribute. A high priority scenario will be one where the implementation cost of the specific GITC-CO is adequate/manageable, resources are available to implement the GITC-CO, and there are no scheduling restrictions. Restrictions is defined as: Costs (C), Availability of Resources (AoR), and Scheduling (T).

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

Organization's Objectives. Refers to the business objectives the GITC-CO satisfies. The higher the number of objectives the GITC-CO satisfies, the higher its priority. Organization's Objectives is defined as: Objective 1 (O1), Objective 2 (O2), …, Objective n (On).

Physical Access. GITC-CO will prevent, detect, and/or record unauthorized changes to the organization's physical location access systems (e.g., building facilities, data centers, accounting department, etc.). The higher the number of physical location access systems

addressed by the GITC-CO, the higher its probability of being selected. Physical Access is defined as: Location 1 (L1), Location 2 (L2), …, Location n (Ln).

Access Controls. Implementation of GITC-CO will promote appropriate levels of computer operations access controls to ensure protection of 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.

Human Resources. Implementation of GITC-CO support reductions of unauthorized access, 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.

Communications and Operations Management. GITC-CO will ensure secure operation of information processing facilities, including adequate segregation of duties (SOD), change management (CM), and network security (NS). Organizations may select GITC-CO to address all of these or just some depending on their particular needs.

Systems Acquisition, Development, and Maintenance. GITC-CO will support security related to the organization's in-house and/or off-the-shelf systems or applications. The higher the number of systems or applications addressed by the GITC-CO, the higher its priority. Systems Acquisition, Development, and Maintenance is defined as: Systems or Applications 1 (SoA1), Systems or Applications 2 (SoA2), …, and Systems or Applications n (SoAn).

Incident Management. This quality attribute ensures that security-related incidents (e.g., attempts to manipulate financial data, etc.) identified are timely communicated and corrected. Incident management may apply to online processing and/or batch processing, and is defined as Processing 1 (P1), Processing 2 (P2), …, and Processing n (Pn).

Results

Using synthetic data for the identified quality attributes and features, an input matrix is generated with synthesized weights for the features of the 10 GITC-CO. Table 1 presents the synthesized weights and corresponds to the input matrix *X* in Equation (3.4). The weights represent the weight vector shown in Equation (3.5) after applying Equations (3.6) - (3.8) on each grey number.

Table 1. Decision matrix and synthesized weights after feature aggregation.

GITC-CO	QA1 = Restrictions Addressed			QA2 = Scope			QA3 = Organization's Objectives			QA4 = Physical Access			QA5 = Access Controls		
	C	AoR	T	S1	S2	Sn	O1	O2	On	L1	L2	Ln	N	O	A
	l		u	l		u	l		u	l		u	l		u
1	3.66		10.05	3.57		13.69	4.46		11.78	7.50		10.39	4.71		10.15
2	4.25		13.41	6.39		10.64	6.95		16.35	5.04		15.23	4.84		7.96
3	5.70		13.73	3.94		12.29	2.74		13.93	4.87		9.30	2.42		12.95
4	3.17		9.49	6.77		10.60	6.98		15.99	5.38		13.73	6.20		12.54
5	5.81		8.81	4.20		11.45	3.87		13.54	5.19		16.46	2.39		11.44
6	6.34		13.72	5.45		12.22	3.61		9.74	8.11		16.23	3.39		16.55
7	3.52		16.53	2.53		10.50	2.20		11.46	3.48		16.45	3.61		6.81
8	4.12		16.44	6.49		12.12	5.98		16.94	3.56		7.91	7.01		13.87
9	3.95		10.92	4.80		15.80	2.56		14.56	4.34		10.43	6.06		14.91
10	8.59		15.22	5.85		14.01	4.34		12.08	4.48		10.23	7.64		14.24
Wj	0.111			0.039			0.118			0.134			0.136		

Table 1. Decision matrix and synthesized weights after feature aggregation. (Cont'd)

GITC-CO	QA6 = Human Resources			QA7 = Communications and Operations Management			QA8 = Systems Acquisition, Development, and Maintenance			QA9 = Incident Management		
	Aw	Tn	E	SOD	CM	NS	SoA1	SoA2	SoAn	P1	P2	Pn
	l		u	l		u	l		u	l		u
1	2.09		7.42	7.87		11.06	2.69		19.10	4.46		9.92
2	6.20		15.73	5.12		14.44	7.29		11.47	3.24		8.97
3	5.34		12.54	3.83		14.06	6.24		12.46	5.15		12.61
4	3.81		16.42	4.46		15.54	1.43		10.60	5.24		13.34
5	3.84		8.88	8.00		17.36	3.16		16.40	5.00		9.57
6	4.27		14.23	4.60		12.28	6.20		12.21	2.67		8.30
7	4.58		11.30	3.03		9.02	3.43		11.39	2.85		12.90
8	5.67		17.18	3.00		9.31	2.86		12.00	4.35		9.04
9	5.91		18.49	7.03		15.28	6.97		13.18	2.69		16.23
10	6.68		13.91	6.60		11.27	7.04		10.95	3.78		8.53
Wj	0.183			0.139			0.073			0.067		

Table 2 corresponds to the normalized *R* matrix after applying Equations (3.9) and (3.10) on each number in the matrix. Ideal GITC-CO are also shown here corresponding to the vector r_0 of Equation (3.11) after applying Equations (3.12) and (3.13) on each column of the Table 2.

Table 2. Normalized matrix and ideal GITC-CO.

GITC-CO	QA1 = Restrictions			QA2 = Scope			QA3 = Organization's Objectives			QA4 = Physical Access			QA5 = Access Controls		
	C	AoR	T	S1	S2	Sn	O1	O2	On	L1	L2	Ln	N	O	A
	i		u	l		u	l		u	l		u	l		u
1	0.005		0.013	0.002		0.006	0.006		0.016	0.011		0.253	0.008		0.016
2	0.005		0.017	0.003		0.005	0.009		0.022	0.018		0.308	0.008		0.013
3	0.007		0.017	0.002		0.006	0.004		0.018	0.007		0.240	0.004		0.021
4	0.004		0.012	0.003		0.005	0.009		0.021	0.008		0.291	0.010		0.020
5	0.007		0.011	0.002		0.005	0.005		0.018	0.008		0.322	0.004		0.018
6	0.008		0.017	0.002		0.005	0.005		0.013	0.012		0.319	0.005		0.027
7	0.004		0.021	0.001		0.005	0.003		0.015	0.005		0.322	0.006		0.011
8	0.005		0.021	0.003		0.005	0.008		0.022	0.005		0.224	0.011		0.022
9	0.005		0.014	0.002		0.007	0.003		0.019	0.007		0.253	0.010		0.024
10	0.011		0.019	0.003		0.006	0.006		0.016	0.007		0.251	0.012		0.023

Table 2. Normalized matrix and ideal GITC-CO. (Cont'd)

GITC-CO	QA6 = Human Resources			QA7 = Communications and Operations Management			QA8 = Systems Acquisition, Development, and Maintenance			QA9 = Incident Management		
	Aw	Tn	E	SOD	CM	NS	SoA1	SoA2	SoAn	P1	P2	Pn
	l		u	l		u	l		u	l		u
1	0.004		0.263	0.017		0.037	0.002		0.016	0.004		0.009
2	0.012		0.353	0.022		0.041	0.006		0.009	0.003		0.008
3	0.011		0.319	0.021		0.032	0.005		0.010	0.005		0.011
4	0.008		0.361	0.024		0.024	0.001		0.009	0.005		0.012
5	0.008		0.279	0.026		0.049	0.003		0.013	0.004		0.009
6	0.008		0.337	0.019		0.029	0.005		0.010	0.002		0.007
7	0.009		0.305	0.014		0.032	0.003		0.009	0.003		0.012
8	0.011		0.369	0.014		0.062	0.002		0.010	0.004		0.008
9	0.012		0.383	0.023		0.033	0.006		0.011	0.002		0.015
10	0.013		0.334	0.017		0.049	0.006		0.009	0.003		0.008

Finally, Table 3 shows the Euclidian distance of each GITC-CO implementation from the ideal GITC-CO, 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 (3.15) and (3.16) on each row of Table 1.

Table 3. Euclidian distances, relational grades, and rankings of all GITC-CO.

GITC-CO	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

As Table 3 shows, the best GITC-CO to implement is GITC-CO 4 (100%), followed by GITC-CO 2 (99.1%) and GITC-CO 9 (98.4%).

Discussion

The research in this paper presents a methodology that uses GST to create a unified measurement that represents how well GITC-CO meet quality attributes and their related features. Through a case evaluation, the approach is proven successful in providing a way for measuring the quality of any number of GITC-CO consistent with organizational goals and objectives. The developed approach is very much appropriate in this particular context given the high visibility and significance of internal controls to organizations, managers, accountants, investors, and the public in general. Selecting and implementing the right internal controls, based on the AICPA (2014), "reduce the risk of asset loss, and help ensure that plan information is complete and accurate, financial statements are reliable, and the plan's operations are conducted in accordance with the provisions of applicable laws and regulations." (p. 3) As evidenced, the methodology developed herein provides for an effective internal control structure not only by addressing the weaknesses identified in traditional assessment methodologies (refer to Section 2), but also by carefully and precisely ranking relevant internal controls (i.e., GITC-CO), resulting in a more accurate control selection and implementation. A major advantage or benefit for organizations from having an approach that prioritizes the selection and implementation of internal controls, as it is the case in this research, is to provide reasonable assurance and consistency with organization's financial reporting strategies, goals, and/or objectives (AICPA, 2014).

There are several important contributions from this research. First, the methodology is readily available for implementation using a spreadsheet or software tool and promote usage in practical scenarios where highly complex methodologies are impractical. Second, the methodology fuses multiple-attribute assessment criteria and features to provide a holistic view of the overall GITC-CO quality. Third, the methodology is easily extended to include additional attributes and features (possibly the most meaningful contribution from this research). Finally, the methodology provides a mechanism to evaluate the quality of GITC-CO in various domains. Overall, the methodology developed and presented in this research proved to be a feasible technique for assessing GITC-CO in organizations.

The authors understand and realize the benefits of testing the developed approach in a real-world setting environment. Only after implementation in a real-world setting will the true

benefits and/or limitations of the proposed approach be exhibited. However, as evidenced in the literature review presented in Section 2, it is not uncommon for controls related to information systems computer operations to be assessed and tested using case evaluations as opposed to real-world setting scenarios. In this research, a case evaluation was used with simulated data representing real-life operational data in order to validate how the proposed approach would be well-suited in most organizational settings. The developed approach proved successful in providing a way for measuring the quality of GITC-CO in protecting accounting information.

Conclusion

The research presented develops an innovative approach for evaluating the quality of GITC-CO in organizations based on a multiple-attribute assessment criteria. Opportunities for future work exist that can enhance the proposed GITC-CO evaluation process. For instance, traditional methodologies nor our proposed solution consider the true degree of relevance (imprecise in nature) when evaluating GITC-CO. The above still represents a major problem for organizations that can potentially impact the overall security over their sensitive accounting information.

An assessment methodology that accounts for organizations' goals while adequately modeling imprecise parameters can guarantee an effective selection of GITC-CO. 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 GITC-CO using FST will lead to a thorough, more detailed assessment, thus, supporting a more effective GITC-CO evaluation. Moreover, based on the literature reviewed, there have not been a research study that specifically evaluated and prioritized organizations' GITC-CO using FST.

While grey numbers can handle easily ambiguous and imprecise data, grey systems still do not provide the 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 GITC-CO. A GITC-CO assessment methodology based on FST provides benefits and advantages over traditional methods, including a strict mathematical methodology that can precisely and rigorously examine vague conceptual phenomena (Zimmermann, 2010). Additionally, FST has been used as a modeling, problem solving, and data mining tool, and has proven superior to existing methods as well as attractive to enhance classical approaches.

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

References

AICPA. (2014). The importance of internal control in financial reporting and safeguarding plan assets. The American Institute of Certified Public Accountants. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/employeebenefitplanauditq

uality/resources/planadvisories/downloadabledocuments/plan-advisoryinternalcontrol-hires.pdf

Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security, 77*(1), 565-577.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems, 5*(1), 2-9.

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.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys, 25*(1), 375-414.

Bettaieb, S., Shin, S. Y., Sabetzadeh, M., Briand, L., Nou, G., & Garceau, M. (2019) Decision Support for Security-Control Identification Using Machine Learning. In: Knauss E., Goedicke M. (eds) Requirements Engineering: Foundation for Software Quality. REFSQ 2019. Lecture Notes in Computer Science, vol 11412. Springer, Cham.

Centrify. (2019). Primary attack points for data breaches in the United States as of 2018 [Graph]. In Statista. Retrieved from https://www-statista-com.portal.lib.fit.edu/statistics/1015959/united-states-primary-attack-points-data-breaches/

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., & 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's Risk Advisory. (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 September 2019).

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(1), 293-314.

Donelson, D. C., Ege, M. S., and McInnis, J. M. (2017). Internal control weaknesses and financial reporting fraud. Auditing: A Journal of Practice & Theory, 45-69.

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

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.

Hevner, A. R., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105.

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).

Jee, D. H., & Kang, K. J. (2000). A method for optimal material selection aided with decision making theory. *Materials & Design, 21*, 199–206.

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 volume 2, 2019.

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

Kuhn, J., Ahuja, M., & Mueller, J. (2013). An examination of the relationship of IT control weakness to company financial performance and health, *International Journal of Accounting & Information Management, 21*(3), pp. 227-240.

Kuhn, J., & Morris, B. (2017). IT internal control weaknesses and the market value of firms. *Journal of Enterprise Information Management, 30*(6), pp. 964-986. https://doi.org/10.1108/JEIM-02-2016-0053

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

Lin, Y.-H., Lee, P.-C., & 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*(1), 115–123.

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

Nachin, N., Tangmanee, C., and Piromsopa, K. (2019). *How to Increase Awareness*. ISACA Journal volume 2, 2019.

Otero, A. R. & Fink, R. P. (2020). Robotic Process Automation to Aid Accounting and Finance Departments. *ISACA Journal, 6*(1), 1-8.

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.

Otero, A. R., Sonnenberg, C., & Delgado-Perez, I. (2020). Change Management Over Financial Information: A Multi-Criteria Evaluation of System Change Controls Using Desirability Functions. *Communications of the IIMA, 18*(1), 1-26.

Otero, A. R. (2019a). Optimization Methodology for Change Management Controls Using Grey Systems Theory. *International Journal of Business and Applied Social Science, 5*(6), 41-59.

Otero, A. R. (2019b). System Change Controls: A Prioritization Approach Using Analytic Hierarchy Process. *International Journal of Business and Applied Social Science, 5*(8), 56-68.

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.

Otero, A. R. (2018). *Information Technology Control and Audit, 5th Edition*. Boca Raton, FL. CRC Press and Auerbach Publications.

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. (2014). An Information Security Control Assessment Methodology for Organizations. (Doctoral dissertation). Nova Southeastern University, Fort Lauderdale, FL. 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., Otero, C. E., & Qureshi, A. (2010). A multi-criteria evaluation of information security controls using Boolean features. *International Journal of Network Security & Its Applications, 2*(4), 1-11. doi:10.5121/ijnsa.2010.2401.

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.

Ponemon, L. (2016). 2016 Ponemon Cost of Data Breach Study, Ponemon Institute sponsored by IBM Corporation, Traverse City, MI, available at: www-03.ibm.com/security/data-breach/ (Accessed September 2019).

Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal of Accounting Information Systems, 20*(1), 38-64.

Rao, R. V., & Patel, B. K. (2010). A subjective and objective integrated multiple attribute decision making method for material selection. *Materials & Design, 31*(1), 4738-4747.

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

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

Shanian, A., & 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*(1), 1095–1104. doi:10.1016/j.jpowsour.2005.12.092.

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.

SOX & Internal Controls Professionals Group. (2017). 2017 State of the SOX/Internal Controls Market Survey.

Thomé, J., Shar, L. K., Bianculli, D., & Briand, L. (2018). Security slicing for auditing common injection vulnerabilities, *Journal of Systems and Software, 137*(1), 766-783.

Tucker, I. (2018). Getting a Better Handle on Compliance and Controls. Strategic Finance, [online] Available at: https://sfmagazine.com/post-entry/december-2018-getting-a-better-handle-on-compliance-and-controls/ [Accessed June 2019].

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 Edition*. Upper Saddle River, NJ: Pearson Prentice Hall, Inc.

Yamaguchi, D., Li, G. D., Mizutani, K., Akabane, T., Nagai, M., & Kitaoka, M. (2006). On the generalization of grey relational analysis. *Journal of Grey System, 9*(1), 23-34.

Yamaguchi, D., Li, G. D., & Nagai, M. (2005). New grey relational analysis for finding the invariable structure and its applications. *Journal of Grey System, 8*(1), 167-178.

Yoon, K. P., & 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., & 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.