International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/

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

System Change Controls: A Prioritization Approach Using Analytic Hierarchy Process

Angel R. Otero[1]
Nathan M. Bisk College of Business
Florida Institute of Technology
150 West University Blvd.
Melbourne, FL 32901
Email: aotero@fit.edu
Office: 321-674-8782
USA

Abstract

Information attacks are a constant threat to every organization. To protect their sensitive information, organizations implement general information technology controls. An example of such controls includes system change controls (or change management controls), which are critical in ensuring the integrity, completeness, and reliability of financial information. The literature points to various evaluation methods of these controls to determine which ones to implement. The literature further shows how traditional assessment methods do not necessarily promote an effective evaluation, prioritization, and, therefore, implementation of system change controls in organizations. Alarming facts within the literature trigger analyses and identification of additional methods to assist organizations in protecting their sensitive and critical information. This research proposes a quantitative approach to assist management in evaluating system change controls using the Analytic Hierarchy Process. Through a case study, the approach is proven successful in providing a way for measuring the quality of system change controls in organizations.

Keywords: System change controls, change management, general IT controls, analytic hierarchy process, quality, evaluation, pairwise comparisons

1. Introduction

The increasing complexity of information technology (IT) environments, attacks on sensitive information, and the implementation of new laws and regulations have all shifted the focus of internal controls in organizations. Nowadays, organizations require internal controls to be designed and implemented effectively and in compliance with laws and regulations (Lavion, 2018). Internal controls refer to the activities and procedures put in place by the organization to mitigate risks that could prevent a company from achieving its business objectives (Deloitte, 2018; GTAG 8, 2009).

Business goals and objectives, such as the reliability of the entity's financial reporting, the effectiveness, and efficiency of its operations, and the compliance with pertinent laws and regulations are common and constantly threatened (Otero, 2018; Otero, Ejnioui, Otero, & Tejay, 2011). Internal controls should be implemented and monitored to ensure business goals and objectives are achieved, and potential concerns regarding the organization's going concern is reduced or eliminated (Otero, Tejay, Otero, & Ruiz, 2012).

Internal controls related to IT (also known as General IT Controls (GITC)) aid in the safeguarding of business operations, particularly, by securing the integrity, completeness, and reliability of financial information, as well as of any other system functionality underlying business processes (Deloitte, 2018; Otero, 2015). GITC refer to policies and procedures that support the effective functioning of applications, including the operation of automated controls embedded in the applications, the integrity of reports generated from the applications, and the security of data hosted within the applications. Based on Deloitte (2018) and Cooke (2019), effective operation of GITC is

[1] Angel R. Otero, Email: aotero@fit.edu (Corresponding Author)

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/
©Center for Promoting Education and Research

critical and of utmost importance to major company's stakeholders (e.g., owners, investors, regulators, audit committees, management, auditors, etc.) for the following reasons:

- Business processes and controls over financial information are constantly relied upon by stakeholders to manage the business and make strategic decisions.
- The effective operation of controls around the company's IT environment ensures adequate processing and reporting of financial data, as well as compliance with applicable laws and regulations.
- Reliance on automation of business processes and financial transactions is becoming increasingly important.
- Cybersecurity is a broad business risk which extends to financial information.

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

GITC commonly include controls over (1) data center and network operations; (2) access security; and (3) change management. Change management includes controls around the areas of system software acquisition, change and maintenance, program change, and application system acquisition, development, and maintenance (Otero, 2018). These controls altogether are collectively referred to as system change controls (SCC).

SCC is critical in ensuring the accuracy and completeness of financial information (Keef, 2019; Otero, 2015; GTAG 2, 2012; Otero, Tejay, Otero, & Ruiz, 2012; Ejnioui, Otero, Tejay, Otero, & Qureshi, 2012). They help minimize the likelihood of disruption, unapproved changes, and errors (ITIL,2016). SCC include controls over each of the relevant technology elements within an entity's IT environment: application system, database, operating system, and network. Examples of SCC include change request approvals; application and database upgrades; and network infrastructure monitoring and security; among others. Given the significance and rapid integration of IT systems with business processes, SCC must be implemented to maintain the completeness and accuracy of the information, as well as the reliability of business processes within the organization.

1.1 Current IT Environment

Throughout the years, organizations have suffered numerous system losses, directly impacting one of their most valuable asset, information. Schwartz (1990) predicted that losses related to confidential and sensitive information will continue to occur with a devastating effect on organizations. Examples of information losses suffered by organizations result from corporate fraud (i.e., white-collar crime), from altering and/or acquiring unauthorized access, from injecting malicious code, and from the inappropriate implementation of changes. The aforementioned likely triggers unreliable processing, incomplete recording of data, lost data, inaccurate calculations, cutoff errors, and other misstatements of the accounting records (ISACA, 2011; Otero, 2015). To that effect, the American Institute of Certified Public Accountants (AICPA) estimates that cybercrime's global cost, which includes financial information losses, will reach $6 trillion by 2021 (Morgan, 2017).

According to the Federal Bureau of Investigation's (FBI) (2019), white-collar crime continues to be one of the highest criminal priorities. Corporate fraud results in significant financial losses to companies and continues causing immeasurable damage to the U.S. economy and investor confidence. FBI (2019) states that the majority of corporate fraud cases pursued mostly involve accounting schemes like false accounting entries; misrepresentations of financial condition; fraudulent trades designed to inflate profits or hide losses; and/or illicit transactions designed to evade regulatory oversight.

The above schemes are designed to deceive investors, auditors, and analysts about the true financial condition of a business entity. Through the manipulation of financial data, share price, or other valuation measurements, the financial performance of a corporation may remain artificially inflated based on fictitious

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/

performance indicators provided to the investing public. To add to the above, in a Global Economic Crime Survey performed by PricewaterhouseCoopers LLP (2014), the views of more than 5,000 participants from over 100 countries were featured on the prevalence and direction of economic crime since 2011. The survey revealed that 54% of U.S. participants reported their companies experienced fraud or inconsistencies with their financial systems over $100,000 with 8% reporting fraud over $5 million. Moreover, the use of web applications has also brought in security risks and vulnerabilities around financial information creating significant exposure for many organizations (ISACA, 2011; Thomé, Shar, Bianculli, & Briand, 2018). An example of the above involved the shutdown of a popular cloud-based tax and accounting software, which had been compromised and ultimately closed down as a result of a malware attack (Ryan,2019). The alarming facts and figures above all point to inadequacy in today's IT environment and serve as motivation for finding new ways to help organizations improve their capabilities for securing, managing, and controlling valuable information.

Currently, most of the challenges related to change management practices are addressed through software tools and technologies (Singh, Picot, Kranz, Gupta, & Ojha, 2013; Volonino & Robinson, 2004; Vaast, 2007). However, it is argued that these tools and technologies alone are not sufficient to address the change management software problems just presented (Keef, 2019; Herath & Rao, 2009). To improve overall change management practices, organizations must evaluate and put in place adequate SCC that satisfy their specific security requirements (Otero, 2019; Barnard & Von Solms, 2000; Da Veiga & Eloff, 2007; Karyda, Kiountouzis, & Kokolakis, 2004). However, due to a variety of organizational-specific constraints like costs, scheduling, resources availability, etc., organizations do not have the luxury of implementing all required SCC. As a result, the implementation of SCC within organizations' business constraints becomes a non-trivial task.

This research proposes a novel approach for evaluating the most appropriate SCC based on organization-specific criteria. The remainder of the paper is organized as follows. Section 2 reviews the literature on previous SCC evaluation approaches in organizations. Section 3 then describes the proposed solution approach. Section 4 presents a case study and its results. Section 5 finalizes with summarized conclusions, contributions, and opportunities for expanding this research.

2. Literature Review

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

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 consistent with the specific needs of the organization. Identification and implementation of the most effective controls is a major step towards providing an adequate IT environment in organizations (Barnard & Von Solms, 2000).

2.1 Previous Evaluation Approaches of SCC in Organizations

Based on Barnard and Von Solms (2000), the process of selecting the most effective SCC in organizations has been a challenge in the past, and plenty of attempts have been made to come up with the most effective way possible. Risk analysis and management (RAM) is 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 with the proposed SCC to mitigate the risks resulting from the analyses and assessments performed.

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/
©Center for Promoting Education and Research

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 performing RAM, organizations may identify 50 change management-related risks. Management, however, may not be able to select and implement all necessary SCC to address the previously identified 50 risks due to costs and scheduling constraints. Moreover, there may not be enough resources within the organization to implement these SCC. In this case, management should list all those risks identified and determine how critical each risk is to the organization while considering costs versus benefits analyses. Management must, therefore, explore new ways to determine and measure the relevance of these SCC considering the constraints just presented.

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

The process of selecting the most effective set of SCC from best practice frameworks can be challenging (Van der Haar & Von Solms, 2003). Van der Haar and Von Solms (2003) state that best practice frameworks leave the choosing of controls to the user while offering little guidance in terms of determining the best controls to provide adequate protection for the particular business situation. Additionally, frameworks do not take into consideration organization-specific constraints, such as costs of implementation, scheduling, and resource constraints. Other less formal methods used in the past, such as ad hoc or random approaches, could lead to the inclusion of unnecessary controls and/or exclusion of required/necessary controls (Barnard and 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). 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 certainly affect the selection of SCC.

In another study, Gerber and von Solms (2008) created a Legal Requirements Determination Model (LRDM) for defining legal requirements, which in turn, indicated relevant SCC 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 SCC 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 SCC from the ISO/IEC 27002 framework was produced to satisfy the previously identified legal requirements.

Nonetheless, as evidenced earlier, the selection of SCC 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). However, baseline manuals or frameworks do not necessarily take into consideration organization-specific constraints like costs, scheduling, and resource constraints, among others.

Completion of checklists is another method used by organizations to identify and select SCC. Chen and Yoon (2010) used checklists as a framework to identify information security risks and common controls within a cloud-based organization. They completed checklists for the Infrastructure-as-a-Service (IaaS) and Software-as-a-

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/
©Center for Promoting Education and Research

Service (SaaS) delivery service models within a public cloud. Results from those checklists were used by internal and external auditors to assess and assure the security of the cloud-based computing environment. Baskerville (1993) states that numerous information security checklists, such as the above, have been proposed and used over the years. Their importance, based on 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). Dhillon and Torkzadeh (2006), nonetheless, 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 of information security managers conducted by Dhillon and Torkzadeh (2006), checklists are not considered to be the essence of information security. Even though checklists may be viewed as good means to ensure information security, exclusively relying on them could result in a flawed information systems security strategy (Dhillon & Torkzadeh, 2006). To add to the above, 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), an innovative control evaluation and selection approach, particularly of controls related to information security, was developed to help decision-makers select the most effective ones in resource-constrained environments. The approach was developed based on functions which quantified the desirability of each control after considering advantages and disadvantages. The evaluation gave management a better picture of each control and, most importantly, provided a measurement that was representative of the overall quality of each security control based on organizational goals. The approach proved successful in providing a way for measuring the quality of controls in organizations. Otero et al.'s (2010) methodology considered controls' relevant quality attributes to determine their relative importance to the 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 information security control was evaluated against each feature using a simple binary scale (0 or 1). Information 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 information security controls met quality attributes, and how important those quality attributes were for the organization. Nevertheless, Boolean criteria for evaluating the quality attributes of each security control may not be considered a precise enough assessment for selecting and ultimately implementing information security controls in organizations.

As seen from the above-reviewed literature, weaknesses are evident in current evaluation approaches (or methodologies) of SCC in organizations. An approach that addresses or enhances the above weaknesses is much needed in the change management security literature. To properly evaluate the quality and priority of SCC, organizations must follow an approach that considers attributes and features that are unique to SCC and, most importantly, relevant to the organization. The next section will discuss the process to develop the proposed evaluation approach.

3. Solution Approach-Analytical Hierarchy Process

To properly evaluate the quality and priority of SCC, organizations must follow an approach that considers attributes and features that are unique to SCC and, most importantly, relevant to the organization. Such an approach must allow management to compare how well SCC perform based on predefined evaluation criteria to determine their relative significance. The approach must also allow management to assign priorities to the evaluation criteria to customize the results based specifically on organization needs. To achieve this, the Analytical Hierarchy Process (AHP) approach created in Otero, Kostanic, and Otero (2010) is modified and customized to solve the problem of prioritizing SCC in organizations. The proposed AHP methodology will compare multiple SCC and determine the best ones for the organization. In making the comparisons, management can use their quantified judgment about the relative meaning and importance of each SCC. The output provided can be used as a unified measurement of the SCC as perceived by management.

AHP is a multi-attribute, decision-making method used to facilitate decisions that involve multiple competing goals (de Steiguer, Duberstein, & Lopes, 2003). It provides a powerful tool that can be used to assess

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/

different SCC based on multiple quality evaluation criteria (QEC). AHP starts by transforming the quality evaluation problem into a structured hierarchy where each QEC is quantified and related to overall goals for evaluating alternative solutions. Common QEC for organizations includes compliance with restrictions (e.g., costs, resource availability, etc.), access security (e.g., logical security, access reviews, etc.), and human resources programs (e.g., employee education and awareness programs on theft, fraud, misuse of computer resources, etc.). Typical goals for evaluating alternative solutions include maximizing (or minimizing) all QEC identified. In all cases, AHP can be used to quantify and prioritize goals. A generic AHP hierarchy for the quality evaluation process for SCC is presented in Figure 1.

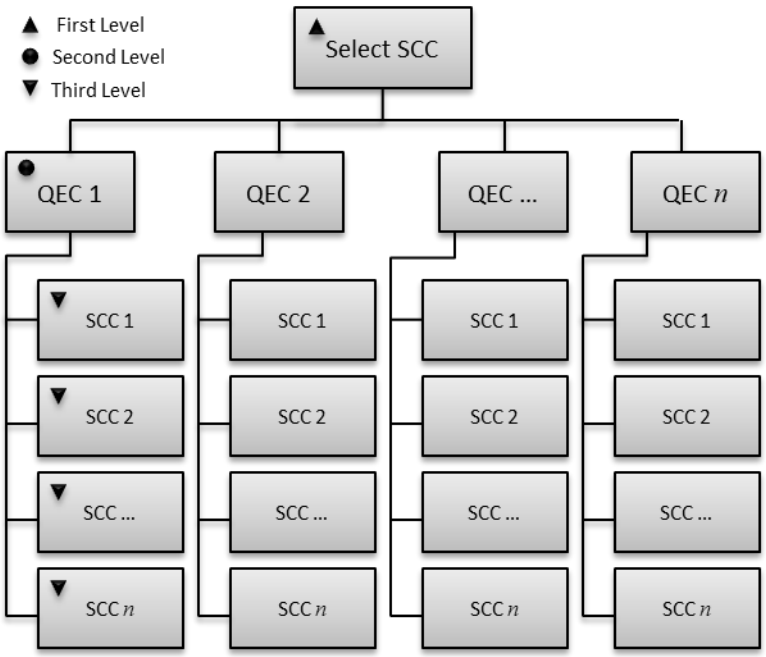

Figure 1. AHP hierarchy for SCC evaluation

The second and third levels of the AHP hierarchy vary according to the SCC available and the QEC selected for evaluation. The second level can be extended to include other QEC, such as, scope (i.e., the required number of systems the SCC should provide security too); the organization objectives that must be met by the SCC; and which physical access locations are to be protected with the SCC. The third level consists of the actual SCC being evaluated. For purposes of this research, three SCC will be considered, SCC1, SCC2, and SCC3. In other scenarios, there could be *n* SCC, each providing different measurements for each QEC identified. Once the hierarchy is built, and relevant QEC measurements were taken for each SCC, a common scale is created to rank each SCC. That is, for each comparison made during the AHP, a common, pair-wise comparison scale is used to determine how preferred one option is from another. This allows standardization in all comparisons made during the AHP process. Table I presents the pairwise comparison scale created for the quality evaluation problem.

Table I. Pairwise comparison scale

Scale (*w*)	Description
1	Equally Preferred
2	Equally to Moderately Preferred
3	Moderately Preferred
4	Moderately to Strongly Preferred
5	Strongly Preferred

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/

©Center for Promoting Education and Research

Quality evaluators establish preferences between different SCC using the pairwise comparison scale and pairwise comparison matrices (de Steiguer, Duberstein, & Lopes, 2003). There are two types of pairwise comparison matrices in AHP, the SCC vs. SCC matrices, and the QEC vs. QEC matrix. The SCC vs. SCC pairwise comparison matrices are $n \times n$ matrices where each element a_{ij} represents how much more desirable the SCC at row i is than the SCC at column j in terms of a pre-defined QEC. The format of the SCC vs. SCC matrices is presented in (1), where A_z is the pairwise comparison matrix for QEC z (i.e., $z \in$ {restrictions, access security, human resources}) and I_x represents SCC x.

$$A_z = \begin{array}{c} \\ I_1 \\ I_2 \\ \vdots \\ I_n \end{array} \begin{array}{c} \begin{array}{cccc} I_1 & I_2 & \cdots & I_n \end{array} \\ \begin{bmatrix} w_1/w_1 & w_1/w_2 & \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \cdots & w_2/w_n \\ \vdots & \vdots & \ddots & \vdots \\ w_n/w_1 & w_n/w_2 & \cdots & w_n/w_n \end{bmatrix} \end{array} \quad (1)$$

From each A_z matrix, a weight vector W is computed to determine the relative importance of each SCC in the pairwise comparison matrix. That is, assuming weight vector $W = [w_1 \quad w_2 \quad \cdots \quad w_n]$, the value of w_i represents the relative importance of SCC i of the associated pairwise comparison matrix based on QEC z. The weight vectors are used to make the final decision. To compute the weight vectors, the pairwise comparison matrix A_z is normalized using (2),

$$A_{norm} = \begin{bmatrix} \frac{a_{11}}{\sum_{i=1}^{n} a_{i1}} & \cdots & \frac{a_{1n}}{\sum_{i=1}^{n} a_{in}} \\ \vdots & \ddots & \vdots \\ \frac{a_{n1}}{\sum_{i=1}^{n} a_{i1}} & \cdots & \frac{a_{nn}}{\sum_{i=1}^{n} a_{in}} \end{bmatrix} \quad (2)$$

where a_{ij} represents the a^{th} element at row i and column j of the respective SCC vs. SCC comparison matrix. Once in normalized form, the weight vector associated with A_{norm} is computed with (3).

$$W = \begin{bmatrix} w_1 = \frac{\sum_{j=1}^{n} a_{1j}}{n} & w_2 = \frac{\sum_{j=1}^{n} a_{2j}}{n} & \cdots & w_n = \frac{\sum_{j=1}^{n} a_{nj}}{n} \end{bmatrix} \quad (3)$$

The QEC vs. QEC pairwise comparison matrix is a $n \times n$ matrix where each location a_{ij} represents how much more important the QEC (i.e., restrictions, access security, and human resources) at row i is than the QEC at column j. The importance of each QEC is configured strictly based on management's goals and objectives. The format of the QEC vs. QEC matrix is presented in (4), where w_i is the weight given to QEC i.

$$A = \begin{array}{c} \\ Q_1 \\ Q_2 \\ \vdots \\ Q_n \end{array} \begin{array}{c} \begin{array}{cccc} Q_1 & Q_2 & \cdots & Q_n \end{array} \\ \begin{bmatrix} w_1/w_1 & w_1/w_2 & \cdots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \cdots & w_2/w_n \\ \vdots & \vdots & \ddots & \vdots \\ w_n/w_1 & w_n/w_2 & \cdots & w_n/w_n \end{bmatrix} \end{array} \quad (4)$$

After the QEC vs. QEC matrix is created, it is then normalized and the weight vector is computed using the same procedure as in the SCC vs. SCC matrices. Once all weight vectors in the quality evaluation problem have

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/
©Center for Promoting Education and Research

been computed, they are used to determine the SCC that provides the best quality. For example, assuming a quality evaluation problem with *x* number of QEC and *y* number of SCC, the AHP provides *y+1* weight vectors: one (W_A) associated with the QEC vs. QEC pair-wise comparison matrix, and the rest W_i associated with each SCC versus SCC matrix *i*, as illustrated in Figure 2.

$$\begin{matrix} w_1^T \\ \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \end{matrix} \quad \begin{matrix} w_2^T \\ \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \end{matrix} \quad \begin{matrix} w_{\cdots}^T \\ \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \end{matrix} \quad \begin{matrix} w_{y-1}^T \\ \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \end{matrix} \qquad \begin{matrix} w_A^T \\ \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \end{matrix}$$

Figure 2. AHP weight vectors

To compute the relative preference for SCC *i*, we let $W = W_i$, $WA = W_A$, and define S_i as the overall score for SCC *i*. This is presented in (5).

$$S_i = \sum_{k=1}^{n} W_k \left(WA_k\right) \qquad (5)$$

where *k* represents the k^{th} element of vectors *W* and *WA*. Once overall scores are computed for all SCC, the highest score is identified as the SCC providing the best quality, followed by the second highest score, and so on. This prioritized list helps determine the best quality for SCC.

4. Case Study

This section presents the results of a quality evaluation case study using the proposed approach from Section 3. The case study evaluates the quality of any three SCC in organizations (i.e., SCC1, SCC2, and SCC3). For this case study, the identified QEC below was used by Otero, Otero, and Qureshi (2010) and include Restrictions, Access Security, and Human Resources (Otero, Otero & Qureshi, 2010; Da Veiga & Eloff, 2007; Nachin, Tangmanee, & Piromsopa, 2019; and ISACA, 2009).

1. *Restrictions*-There are restrictions that management must consider before selecting SCC, and they may include whether the costs involved in the implementation of the SCC are considered high by the organization, whether resources are not available, and whether there are scheduling constraints associated with implementing the SCC.

2. *Access Security*-Implementation of an SCC will promote appropriate levels of access security to ensure the protection of the organization's systems/applications against unauthorized activities. Organizations may implement network access controls, operating systems access controls, and application (or automated) controls based on their specific needs.

3. *Human Resources*-Implementation of human resources access controls support reductions of risk of theft, fraud, and/or misuse of computer resources by promoting information security awareness, training, and education for employees.

To evaluate the quality provided by the SCC, pairwise comparisons of each SCC in terms of each QEC are performed. Each SCC is compared using the comparison scale specified in Table I. Results are presented below in Tables II, III, and IV.

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/

©Center for Promoting Education and Research

Table II. SCC vs. SCC comparison matrix, normalized matrix, and weight vector for Restrictions

Restrictions	SCC1	SCC2	SCC3
SCC1	1	4	3
SCC2	0.25	1	0.33
SCC3	0.33	3	1
Total	1.58	8	4.33

Restrictions	SCC1	SCC2	SCC3	Total
SCC1	0.63	0.50	0.69	1.82
SCC2	0.16	0.13	0.08	0.37
SCC3	0.21	0.38	0.23	0.82

Restrictions	SCC1	SCC2	SCC3
Weight	0.61	0.12	0.27

Table III. SCC vs. SCC comparison matrix, normalized matrix, and weight vector for Access Security

Access Security	SCC1	SCC2	SCC3
SCC1	1	4	0.25
SCC2	0.25	1	0.20
SCC3	4	5	1
Total	5.25	10	1.45

Access Security	SCC1	SCC2	SCC3	Total
SCC1	0.19	0.40	0.17	0.76
SCC2	0.05	0.10	0.14	0.29
SCC3	0.76	0.50	0.69	1.95

Access Security	SCC1	SCC2	SCC3
Weight	0.25	0.10	0.65

Table IV. SCC vs. SCC comparison matrix, normalized matrix, and weight vector for Human Resources

Human Resources	SCC1	SCC2	SCC3
SCC1	1	0.33	0.20
SCC2	3	1	0.25
SCC3	5	4	1
Total	9	5.33	1.45

Human Resources	SCC1	SCC2	SCC3	Total
SCC1	0.11	0.06	0.14	0.31
SCC2	0.33	0.19	0.17	0.69
SCC3	0.56	0.75	0.69	2.00

Human Resources	SCC1	SCC2	SCC3
Weight	0.10	0.23	0.67

Using the pairwise comparison matrices of all SCC based on each QEC, the AHP can now be used to compute a measurement of quality for each SCC.

International Journal of Business and Applied Social Science
EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/
©Center for Promoting Education and Research

To properly reflect the relative importance of each QEC, QEC vs. QEC comparisons are made. The QEC vs. QEC comparison matrix, normalized matrix, and weight vector are presented in Table V.

Table V. QEC vs. QEC comparison matrix, normalized matrix, and weight vector

QEC vs. QEC	Restrictions	Access Security	Human Resources
Restrictions	1	4	5
Access Security	0.25	1	4
Human Resources	0.20	0.25	1
Total	1.45	5.25	10

QEC vs. QEC	Restrictions	Access Security	Human Resources	Total
Restrictions	0.69	0.76	0.50	1.95
Access Security	0.17	0.19	0.40	0.76
Human Resources	0.14	0.05	0.10	0.29

	Restrictions	Access Security	Human Resources
Weight	0.65	0.25	0.10

Using (5), the results of Tables II through V are combined to provide the final quality measurement for each SCC evaluated. The final perceived quality measurement is presented in Table VI.

Table VI. SCC final quality measurement

SCC	Quality
SCC1	47.00%
SCC2	12.42%
SCC3	40.57%

As shown, the final quality measurement shows SCC1 (47.00%) as the best performer, followed by SCC3 (40.57%) and SCC2 (12.42%). It is important to note that the evaluation of SCC using this approach is fully dependent on the organization and its particular change management security objectives.

5. Conclusions, Contributions, and Future Research

The literature continues 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, to mention a few. The research presented in this paper develops an innovative approach for evaluating the quality of SCC in organizations based on multiple quality evaluation criteria. The methodology uses AHP to create a unified measurement that represents how well SCC satisfy quality attributes and how important such quality attributes are for the organization. Through a case study, the approach is proven successful in providing a way of measuring and evaluating the quality of SCC for organizations.

The approach presented here fuses unlimited quality evaluation criteria to provide a holistic view of the experienced quality. This allows the approach to be easily extended to include additional quality criteria not considered in this research. Moreover, the approach provides a mechanism to evaluate quality based on specific

EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/

scenarios. By modifying the parameters of the QEC vs. QEC comparison matrix, quality can be evaluated taking into consideration different scenarios. Overall, the approach presented in this research proved to be a feasible technique for effectively evaluating the quality of SCC in organizations.

Opportunities for future research exist that can enhance the proposed solution to improve the overall quality of the SCC selection process. For instance, neither traditional methodologies nor our proposed solution herein considers the true degree of relevance (imprecise in nature) when evaluating SCC. The above still represents a major problem for organizations that can potentially impact overall change management practices over the information. An assessment methodology that accounts for organizations' goals while also models imprecise parameters can guarantee an effective selection of SCC. A further potential research opportunity involves 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.

References

Backhouse, J., and Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems, 5*(1), 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*(1), 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*(1), 337-346.

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).

Cooke, I. (2019). *Auditing Cybersecurity*. ISACA Journal volume 2, 2019. https://www.isaca.org/Journal/archives/2019/Volume-2/Pages/auditing-cybersecurity.aspx?utm_referrer=

Da Veiga, A., and Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(1), 361-372.

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).

de Steiguer, J.E., Duberstein, J., Lopes, V., (2003). The Analytic Hierarchy Process as a Means for Integrated Watershed Management. Available at: http://www.tucson.ars.ag.gov/icrw/Proceedings/Steiguer.pdf [Accessed 5 June 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, 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.

EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/
©Center for Promoting Education and Research

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.

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

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).

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. Pricewaterhouse Coopers LLP, https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html#cta-1 (Accessed May 2019).

Loch, K., Conger, S. and Oz, E. (1998). Ownership, privacy and monitoring in the workplace: A debate on technology and ethics. *Journal of Business Ethics, 17*(1), 653-663.

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.

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. (2019). 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. (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.

EISSN: 2469-6501
VOL: 5, ISSUE:8
August/2019
DOI: 10.33642/ijbass.v5n8p4
https://ijbassnet.com/
©Center for Promoting Education and Research

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., 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, 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, C. E., Kostanic, I, & Otero, L. D. 2010. "Characterization of User-Perceived QoS using Network Pairwise Comparisons," *Proceedings of 6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, October, 2010.

Post, G. V. and Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, *26*(3), 229-237.

PricewaterhouseCoopers LLP. (2014). *Economic crime: A threat to business globally*. PwC's 2014 Global Economic Crime Survey, Available at: https://www.pwc.at/de/publikationen/global-economic-crime-survey-2014.pdf (Accessed May 2019).

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.

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.

Wood, C. (2000). An unappreciated reason why security policies fail. *Computer Fraud and Security, 10*(1), 13-14.