Communications of the IIMA

Volume 18 | Issue 1 Article 1

Change Management Over Financial Information: A Multi-Criteria Evaluation of System Change Controls Using Desirability Functions

Angel R. Otero
Florida Institute of Technology, aotero@fit.edu

Christian Sonnenberg
Florida Institute of Technology

Ivonne Delgado-Perez
Florida Institute of Technology

Recommended Citation

Otero, Angel R.; Sonnenberg, Christian; and Delgado-Perez, Ivonne () "Change Management Over Financial Information: A Multi-Criteria Evaluation of System Change Controls Using Desirability Functions," *Communications of the IIMA*: Vol. 18 : Iss. 1 , Article 1.
Available at: https://scholarworks.lib.csusb.edu/ciima/vol18/iss1/1

Change Management Over Financial Information: A Multi-Criteria Evaluation of System Change Controls Using Desirability Functions

Cover Page Footnote

The authors would like to thank the reviewers for their time and valuable review which contributed favorably to the quality of our manuscript.

Change Management Over Financial Information: A Multi-Criteria Evaluation of System Change Controls Using Desirability Functions

Angel R. Otero
Florida Institute of Technology, USA
aotero@fit.edu

Christian Sonnenberg
Florida Institute of Technology, USA
csonnenb@fit.edu

Ivonne Delgado-Perez
Florida Institute of Technology, USA
idelgado@fit.edu

ABSTRACT

The increasing complexity of information technology, attacks on confidential information, and the passing of new laws and regulations have shifted the focus around internal controls in organizations. Particularly, general information technology controls related to change management (i.e., system change controls) are critical in ensuring the integrity, completeness, and reliability of financial information. The literature points to various evaluation methods for these controls to determine which ones to implement. However, these methods do not necessarily consider relevant organization constraints, preventing the inclusion of required controls or the exclusion of unnecessary controls. This paper proposes a novel approach, using Desirability Functions, for evaluating system change controls providing management with a measurement that is representative of the overall quality of each control based solely on organizational goals and objectives. Through a case assessment, the approach is proven successful in providing a way for measuring the quality of system change controls in organizations.

Keywords: Internal controls, General IT Controls, change management, system change controls, desirability functions

INTRODUCTION

The increasing complexity of information technology (IT), attacks on confidential information, and the passing of new laws and regulations have all shifted the focus around internal controls in organizations. Today, more than ever, organizations require internal controls to be well-designed, implemented, and to operate effectively and in compliance with laws and regulations (Lavion, 2018). Internal controls refer to procedures and activities implemented by management to mitigate the risks that could prevent a company from achieving its business objectives (Deloitte, 2018; GTAG 8, 2019).

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

Internal controls related to IT or General IT Controls (GITC) aid in the protection 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, 2015a). GITC are 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 housed within the applications. Based on Deloitte (2018) and Cooke (2019), effective design, implementation, and operation of GITC are 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, controls, and financial data relevant to financial information are often relied upon by stakeholders in order to manage the business and make strategic decisions.
- Effective operations of controls around the company's IT environment ensure adequate processing and reporting of financial data, as well as compliance with relevant laws and regulations.
- Automation of business processes and financial transactions is becoming increasingly important and relied upon. Automated controls rely on GITC to ensure they function properly.
- Cyber security is a broad business risk which extends to financial information.

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

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

SCC are critical in ensuring the security, integrity, completeness, and reliability of financial information (Keef, 2019; Otero, 2015a; GTAG 2, 2019; Otero, Tejay, Otero, & Ruiz, 2012; Ejnioui, Otero, Tejay, Otero, & Qureshi, 2012). SCC include controls over each of the relevant technology elements within the entity's IT environment, including the 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 in place in order to maintain the completeness and accuracy of information, as well as the reliability of business processes within the organization.

Change Management Process and Challenges

As stated before, change management is one of the three major GITC areas that assess organization's policies and procedures related to application systems in order to support the effective functioning of application controls (Otero, 2018). According to the Information Technology Infrastructure Library Change Management (2016), change management is a process designed to understand and minimize risks while making changes within the IT environment. The objective of change management is to enable the IT environment to allow rapid change while minimizing the possibility of disruption. The decision about whether to approve and implement a proposed IT change is sometimes a strategic one, and therefore it is expected that the change management process be adequately managed and controlled.

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

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

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

A third challenge relates to inadequate segregation of duties. A well-controlled change management process monitors and ensures that there is proper segregation between who initiates the change, who approves the change, who develops the change, and who implements the change in the production environment. Having the same individual with granted access to analyze, design, construct, test, and implement a change in the live environment may result in overlooking errors, implementing incorrect and incomplete changes, etc. Per Otero (2019a) and Otero (2014), individuals with complete access to develop and implement changes into production will trigger many dangerous systems' risks, including but not limited to: unauthorized access to programs or data; unauthorized remote access; inaccurate information; erroneous or falsified data input; incomplete, duplicate, and untimely processing; communications system failure; inaccurate or incomplete output; and insufficient documentation. Segregation of duties certainly plays an important role in the entire change management process and must be effectively controlled.

Current IT Environment

Throughout the years, organizations have experienced numerous system losses which have had a direct impact on their most valuable asset, information. Schwartz (1990) stated that losses related to confidential, sensitive, and/or financial information will continue to happen, and their effect will be devastated to organizations. Examples of information losses suffered by organizations result from fraud and economic crimes (i.e., white-collar crime), from altering and/or acquiring unauthorized access, from injecting malicious code, and from the inappropriate implementation of changes, all of which could result in inaccurate calculations, unreliable processing, incomplete recording of data, lost data, cutoff errors, and other misstatements of the accounting records (ISACA, 2011; Otero, Sonnenberg, & Bean, 2019; Otero, 2019b).

According to the Federal Bureau of Investigation's (FBI) (2019), white-collar crime or corporate fraud continues to be one of the FBI's highest criminal priorities. Corporate fraud results in significant financial losses to companies and investors and continue causing immeasurable damage to the U.S. economy and investor confidence. FBI (2019) states that the majority of corporate fraud cases pursued mostly involve accounting schemes, such as: false accounting entries and/or misrepresentations of financial condition; fraudulent trades designed to inflate profits or hide losses; and/or illicit transactions designed to evade regulatory oversight. The above schemes are designed to deceive investors, auditors, and analysts about the true financial condition of a corporation or business entity (Otero, 2015b). These schemes are often the result of weakly-implemented controls, particularly SCC (Keef, 2019; Otero, 2015a). SCC include controls over relevant technology elements such as financial application systems, databases, operating systems, and networks. Therefore, they must be in place to maintain complete and accurate financial information, as well as to safeguard against any potential manipulation or abuse of such relevant information.

Through manipulation of financial data, share price, or other valuation measurements, financial performance of a corporation may remain artificially inflated based on fictitious performance indicators provided to the investing public.

To add to the above, in a Global Economic Crime Survey performed by PricewaterhouseCoopers LLP (2014), the views of more than 5,000 participants from over 100 countries were featured on the prevalence and direction of economic crime since 2011. The survey revealed that 54% of U.S. participants reported their companies experienced fraud or inconsistencies with their financial systems in excess of $100,000 with 8% reporting fraud in excess of $5 million. Moreover, the use of web applications (which has grown exponentially and benefitted many organizations) has also brought in security risks and vulnerabilities around financial information creating significant exposure for many organizations (ISACA, 2011; Thomé, Shar, Bianculli, & Briand, 2018). The alarming facts and figures above all point to an inadequacy in today's IT environment and serve as motivation for finding new ways to help organizations improve their capabilities for securing, managing, and controlling valuable information.

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

This research proposes a novel approach for evaluating the most appropriate SCC based on organization specific criteria. The proposed approach uses Desirability Functions to quantify the desirability of each SCC taking into account benefits and penalties (restrictions) associated with implementing the SCC. This provides management with a measurement that is representative of the overall quality of each SCC based on organizational goals and objectives. The derived quality measurement can be used as the main metric for selecting SCC.

BACKGROUND WORK

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

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

Previous Approaches in the Selection and Evaluation of SCC in Organizations

Based on Barnard and Von Solms (2000), the process of identifying (and selecting) the most effective SCC in organizations has been a challenge in the past, and plenty of attempts have been made to come up with the most effective way possible. Risk analysis and management (RAM) is just one example. RAM has been recognized in the literature as an effective approach to identify SCC (Barnard & Von Solms, 2000). RAM consists of performing business analyses as well as risk assessments, resulting in the identification of information security requirements (Barnard & Von Solms, 2000). RAM would then list the information security requirements as well as the proposed SCC to be implemented to mitigate the risks resulting from the analyses and assessments performed.

RAM, however, has been described as a subjective, bottom-up approach (Van der Haar & Von Solms, 2003), not taking into account organizations' specific constraints. For example, through performing RAM, organizations may identify 50 change management-related risks. Nonetheless, management 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 individual risk is to the organization, while considering costs versus benefits analyses. Management must, therefore, explore new ways to determine and measure the relevancy of these SCC considering the constraints just presented.

Baseline manuals or best practice frameworks is another approach widely used by organizations to introduce minimum controls in organizations (Barnard & Von Solms, 2000). Saint-Germain (2005) states that best practice frameworks assist organizations in identifying appropriate SCC. Some best practices include: Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL) Change Control, the National Institute of Standards and Technology (NIST), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). Da Veiga and Eloff (2007) have mentioned other best practice frameworks which have also assisted in the identification and selection of SCC. These are: 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 these 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 & Von Solms, 2000). Identifying and selecting SCC based on the above may result in organizations not being able to protect the overall confidentiality, integrity, and availability of their information (Saint-Germain, 2005). In order to increase the effectiveness of the selection and prioritization process for SCC, new methods need to be developed that save time while considering major factors (e.g., constraints, restrictions, etc.) that undoubtedly affect the selection of 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 a 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). Furthermore, baseline manuals or frameworks do not necessarily take into consideration organization specific constraints, such as costs, scheduling, and resource constraints, among others.

SOLUTION APPROACH

To properly evaluate the quality, significance, and priority of SCC in organizations, management must follow a methodology that takes into consideration the quality attributes of the SCC that are considered relevant. The methodology must provide capabilities to determine the relative importance of each identified quality attribute. This would allow the methodology to provide an SCC selection/prioritization scheme that represents how well these SCC meet quality attributes and how important those quality attributes are for the specific organization. To achieve this, the methodology created in Otero, Otero, and Qureshi (2010) is modified and customized to solve the problem of prioritizing SCC in organizations. First, a set of quality attributes are identified as evaluation criteria for all possible SCC. These attributes are defined in terms of different features, where each feature is determined to be either present or not. Once all features are identified, each individual SCC is evaluated against each feature using a simple binary (boolean) scale (i.e., 0 or 1). SCC that satisfy the highest number of features would expose a higher level of quality (or priority) for that particular quality attribute. Once all SCC are evaluated and measurements computed for all features, the proposed approach uses Desirability Functions to fuse all measurements into one unified value that is representative of the overall quality of the SCC. This unified value is computed by using a set of Desirability Functions that take into consideration the priority of each quality attribute. Therefore, the resulting priority of each SCC is derived based on management goals and organization needs. This results in an SCC evaluation/prioritization approach based on how well SCC meet quality attributes and how important those quality attributes are for the organization.

DESIRABILITY FUNCTIONS

Desirability Functions are a popular approach for simultaneous optimization of multiple responses (Derringer & Suich, 1980; Montgomery, 2008). They have been used extensively in the literature for process optimization in industrial settings, where finding a set of operating conditions that optimize all responses for a particular system is desired (Otero, Otero, & Qureshi, 2010). Through Desirability Functions, each system response y_i is converted into an individual function d_i that varies over the range $0 \leq d_i \leq 1$, where $d_i = 1$ when a goal is met, and $d_i = 0$ otherwise (Montgomery, 2008). Once each response is transformed, the levels of each factor are typically chosen to maximize the overall desirability which is represented as the geometric mean of all m transformed responses (Derringer & Suich, 1980). Alternatively, when factors are uncontrollable, the overall desirability value can be used to characterize the system based on the multiple selected criteria.

Similar to the characterization of industrial processes, the evaluation of the quality and prioritization of each SCC in organizations can be approached by finding the set of criteria that provide the optimal benefit versus cost value for a particular organization. When formulated this way, Desirability Functions can be used to provide a unified measurement that characterizes the quality of SCC based on a set of predefined evaluation criteria. Once the desirability of all SCC is computed, management can use this information to determine the relative priority of SCC and select the best ones simply by choosing the most desirable ones for the particular organization.

Computing Desirability

The first step in the Desirability Functions approach involves identifying all possible SCC that could be implemented in an organization. These SCC can be obtained from the best practice frameworks as mentioned earlier. For instance, ITIL Change Control, COBIT, and/or ISO/IEC 27001 and 27002, all offer best practices or controls to help companies ensure that all program/system changes are appropriately managed, minimizing the likelihood of disruption, unauthorized alterations, and errors which may impact the accuracy, completeness, and valid processing and recording of financial information. Once selected, the results of these SCC are captured in the SCC vector, as presented in (4.1).

$$X = \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_n \end{bmatrix} \tag{4.1}$$

Once the SCC vector is identified, each SCC can be evaluated against a set of quality attributes *QA_1, QA_2,.., QA_n*. The evaluation process takes place as follow. First, each quality attribute is defined in terms of m features, where *$m > 1$*. The evaluation scale for each feature is binary; that is, the feature is evaluated as being present/true (i.e., 1) or missing/false (i.e., 0). For example, SCC can be prioritized based on their scope. In other words, SCC that effectively minimize the likelihood of disruption, unauthorized alterations, and errors impacting the accuracy, completeness, and validity of processing and recording of financial information in many systems (i.e., more than one system) have a higher priority than SCC that address the above in a smaller number of systems. In this case, the quality attribute scope can be defined with the following features: *System 1, System 2, ..., System n*. Therefore, the highest priority SCC (based on the scope quality attribute) would be one where *System 1 = 1, System 2 = 1, and System n = 1*. Similarly, the lowest priority SCC based on the scope quality attribute is one where *System 1 = 0, System 2 = 0, and System n = 0*. For quality attributes where the presence of features affects change management practices negatively (e.g., restrictions, penalties, etc.), the reverse is true. In these cases, SCC with all features present (i.e., 1) result in lower priority and SCC with all features missing (i.e., 0) will result in higher priority. With this framework in place, a measurement of the importance of the *j^{th}* SCC based on the *i^{th}* quality attribute (e.g., scope) can be computed using (4.2),

$$y_{ij} = \frac{\sum_{x=0}^{m} f_x}{m} \tag{4.2}$$

where *m* is the number of features identified for the *i^{th}* quality attribute. This computation normalizes the evaluation criteria to a scale of 0 – 100, where 0 represents the lowest score and 100 the highest (backwards for restrictions or penalties). The overall assessment of the SCC set based on all quality attributes is captured using the quality assessment matrix *Q* presented in (4.3). As seen, each *y_{ij}* value of the matrix represents the score of the *j^{th}* SCC based on each individual *i^{th}* quality attribute. It is important to point out that the quality assessment matrix can be extended to evaluate SCC based on any quality attributes containing numerous features.

$$Q = \begin{array}{c} \begin{array}{cccc} QA_1 & QA_2 & \cdots & QA_m \end{array} \\ \begin{bmatrix} y_{11} & y_{21} & \cdots & y_{m1} \\ y_{12} & y_{22} & \cdots & y_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1n} & y_{2n} & \cdots & y_{mn} \end{bmatrix} \end{array} \tag{4.3}$$

Finally, to assess the importance of each quality attribute, a weight vector *W* is created where r_i represents the importance of the QA_i quality attribute using the scale 0 – 10, where 0 represents lowest importance and 10 represents highest importance. The weight vector *W* is presented in (4.4).

$$W = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix} \tag{4.4}$$

Once the information from *X, Q,* and *W* is collected, desirability values for each SCC can be computed using the desirability matrix *d* presented in (4.5). As seen, each d_{ij} value of the matrix represents the desirability of the j^{th} SCC based on each individual i^{ih} quality attribute.

$$d = \begin{bmatrix} d_{11} & d_{21} & \cdots & d_{m1} \\ d_{12} & d_{22} & \cdots & d_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ d_{1n} & d_{2n} & \cdots & d_{mn} \end{bmatrix} \tag{4.5}$$

Each individual desirability value d_{ij} for the SCC is computed according to management based on the organization's specific needs, goals, and objectives. For example, quality attributes that are represented positively by a higher y_{ij} value are transformed using the *maximization* function in (4.6) (Montgomery, 2008). Alternatively, quality attributes that are represented negatively by a higher y_{ij} value are transformed using the *minimization* function in (4.7) (Montgomery, 2008),

$$d_{ij} = \begin{cases} 0 & y_{ij} \le L \\ \left(\dfrac{y_{ij} - L}{T - L} \right)^{r_i} & L \le y_{ij} \le T \\ 1 & y_{ij} > T \end{cases} \tag{4.6}$$

$$d_{ij} = \begin{cases} 1 & y_{ij} < T \\ \left(\dfrac{U - y_{ij}}{U - T} \right)^{r_i} & T \le y_{ij} \le U \\ 0 & y_{ij} > U \end{cases} \tag{4.7}$$

where L and U are the lower and upper limits, respectively, T is the target objective (e.g., 100 for maximization, 0 for minimization), and r_i is the desirability weight for the i^{th} quality attribute. It is important to note that (4.6) and (4.7) are the normal equations for the Desirability Function approach. However, through experimentation, it was found that the approach for SCC selection and prioritization performed better when $d_{ij} > 0$. Therefore, as heuristic, when d_{ij} is less than .0001, the d_{ij} value is set to .0001. A desirability weight of $r = 1$ results in a linear Desirability Function; however, when $r > 1$, curvature is exposed by the Desirability Function to emphasize on being close to the target objective (T). When $0 < r < 1$, being close to the target objective is less important. Once individual desirability values for each quality attribute are computed, the overall SCC desirability value can be computed using (4.8). As seen, each overall desirability value is computed as the geometric mean of all m individual desirability values for SCC $1, 2, \ldots, n$.

$$D = \begin{bmatrix} \left(\prod_{i=1}^{m} d_{i1} \right)^{1/m} \\ \left(\prod_{i=1}^{m} d_{i2} \right)^{1/m} \\ \vdots \\ \left(\prod_{i=1}^{m} d_{in} \right)^{1/m} \end{bmatrix} \tag{4.8}$$

After overall desirability values are computed for all SCC, management can use these values as a priority measurement derived from the predefined quality attributes and their relative importance for the particular organization.

CASE ASSESSMENT

This section presents the results of a SCC evaluation/prioritization case assessment using the proposed approach 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 SCC in order to mitigate risks to financial information. We generated simulated data for cybersecurity quality attributes and features for the input matrix. The simulated data represents real-life operational data from an organization's cybersecurity program. Overall, the case evaluates any 10 SCC based on the following identified quality attributes, some of which have been defined within the ISO/IEC 177995 and 27002 standards (Da Veiga & Eloff, 2007; Nachin, Tangmanee, & Piromsopa, 2019; ISACA, 2009).

1. *Restrictions* – There are restrictions that management must take into account before selecting and implementing SCC. These may include whether the costs involved in the selection and implementation of the SCC are high, whether resources are not available, and whether there are scheduling constraints associated with implementing the SCC. The presence of any of the above will negatively affect the specific quality attribute. That is, SCC with all features present will result in a lower priority; conversely, SCC with all features missing will result in a higher priority. A high priority scenario will be one where the implementation cost of the specific SCC is considered adequate and manageable (e.g., within budget), resources are available to implement the particular SCC, and there are no restrictions in terms of scheduling the SCC (i.e., the SCC can be scheduled anytime during the year). Restrictions is defined as: Costs (C), Availability of Resources (AoR), and Scheduling (T).
2. *Scope* – This quality attribute assesses the impact of the SCC on the organization. SCC that effectively minimize the likelihood of disruption, unauthorized alterations, and errors which impact the accuracy, completeness, as well as validity and recording of financial information in many systems have a higher priority than SCC that address the above in a smaller number of systems. Scope is defined as: System 1 (S1), System 2 (S2), …, System n (Sn).
3. *Organization's Objectives* – Refers to the number of business goals and objectives the SCC satisfies. The higher the number of objectives the SCC satisfies, the higher the desirability of the SCC. Organization's objectives is defined with the following features: Objective 1 (O1), Objective 2 (O2), …, Objective n (On).
4. *Access Controls* – Implementation of an SCC for this quality attribute will promote appropriate levels of change management access controls to ensure protection of the organization's systems and 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.

5. *Human Resources* – Implementation of SCC support reductions of unauthorized access, inadequate change implementations, fraud, or misuse of computer resources by promoting information security awareness (Aw), training (Tn), and education of employees (E). Depending on the particular situation, costs involved, and availability of personnel, organizations may select which of these to employ.
6. *Communications and Operations Management* – SCC will ensure the correct and secure operation of information processing facilities, which includes addressing for adequate segregation of duties (SoD), change management (CM), and network security (NS). Organizations may select SCC to address all of these or just some depending on their particular needs.
7. *Systems Acquisition, Development, and Maintenance* – SCC will support security related to the organization's in-house and/or off-the-shelf systems or applications (e.g., ensure personnel with authorized access can move changes into production environments, etc.). The higher the number of systems or applications addressed by the SCC, the higher the desirability of the SCC. Systems Acquisition, Development, and Maintenance is defined as: Systems or Applications 1 (SoA1), Systems or Applications 2 (SoA2), …, and Systems or Applications n (SoAn).
8. *Incident Management* – Incident Management ensures that security-related incidents (e.g., attempts to change/manipulate financial data, etc.) identified within the organization's processing of information are communicated in a timely manner and that corrective action is taken for any exceptions identified. Incident management may apply to online processing and/or batch processing. Incident Management is defined as Processing 1 (P1), Processing 2 (P2), …, and Processing n (Pn).

Using synthetic data for the identified quality attributes, binary input evaluation (Table 1), and Desirability Functions parameters (Table 2), results were generated from executing the Desirability Functions and presented in Table 3. As seen in Table 2, all lower and upper boundaries are set to 0 and 100, respectively. Also, all quality attributes have been identified as having equal priority. This is accomplished by setting the weight $r = 1$ for all quality attributes. Finally, different target values have been identified for each quality attribute. This means that the threshold for achieving 100% desirability is customized for each quality attribute. For example, quality attributes where $T = 70$ are considered 100% desirable if they exhibit 70% (or more) of the features that define them.

Table 1. Binary Input Evaluation.

	QA1 = Restrictions			QA2 = Scope			QA3 = Organization's Objectives			QA4 = Access Controls		
	C	AoR	T	S1	S2	Sn	O1	O2	On	N	O	A
1	1	0	0	0	1	1	1	0	1	0	0	1
2	0	1	1	1	1	1	0	0	1	1	0	0
3	1	0	1	0	0	0	0	0	0	0	1	0
4	0	1	1	0	1	0	0	1	0	1	0	1
5	0	1	0	0	0	0	0	0	1	1	0	0
6	0	0	0	1	0	1	0	0	0	1	1	1
7	0	1	1	0	0	0	0	1	0	0	1	0
8	1	0	1	0	1	0	1	1	1	1	0	1
9	1	1	1	0	0	1	0	0	0	1	1	0
10	0	0	1	0	1	1	0	0	0	0	1	0

Table 1. Binary Input Evaluation. (Cont'd)

	QA5 = Human Resources			QA6 = Communications and Operations Management			QA7 = Systems Acquisition, Development, and Maintenance			QA8 = Incident Management		
	Aw	Tn	E	SoD	CM	NS	SoA1	SoA2	SoAn	P1	P2	Pn
1	1	0	0	1	0	0	1	0	1	0	1	0
2	1	1	0	0	0	0	0	0	1	1	1	0
3	0	1	1	1	0	1	0	1	0	0	0	1
4	1	0	0	0	0	1	0	0	1	0	0	1
5	1	1	0	1	0	1	1	1	1	1	0	1
6	0	0	0	0	0	1	1	0	0	0	1	0
7	1	0	0	1	0	0	1	0	1	1	0	1
8	1	1	1	1	0	1	1	1	0	0	0	0
9	0	1	0	0	1	0	1	0	1	0	1	1
10	1	0	0	1	1	0	1	1	0	1	0	1

Table 2. Desirability Function Parameters.

	QA1 = Restrictions	QA2 = Scope	QA3 = Organization's Objectives	QA4 = Access Controls
L	0	0	0	0
U	100	100	100	100
T	50	70	100	60
r	1	1	1	1

Table 2. Desirability Function Parameters. (Cont'd)

	QA5 = Human Resources	QA6 = Communications and Operations Management	QA7 = Systems Acquisition, Development, and Maintenance	QA8 = Incident Management
L	0	0	0	0
U	100	100	100	100
T	70	40	40	40
r	1	1	1	1

Table 3. Desirability Function Results.

	QA1 = Restrictions			QA2 = Scope			QA3 = Organization's Objectives			QA4 = Access Controls		
	C	AoR	T	S1	S2	Sn	O1	O2	On	N	O	A
1	1.0000			0.9524			1.0000			1.0000		
2	1.0000			0.4762			0.6667			1.0000		
3	0.6667			0.9524			0.6667			1.0000		
4	1.0000			1.0000			0.3333			0.5556		
5	0.6667			0.9524			0.3333			1.0000		
6	1.0000			0.9524			1.0000			0.5556		
7	0.6667			0.0014			1.0000			1.0000		
8	0.6667			0.9524			0.6667			1.0000		
9	0.6667			0.4762			0.3333			1.0000		
10	0.6667			0.4762			0.3333			1.0000		

Table 3. Desirability Function Results. (Cont'd)

	QA5 = Human Resources			QA6 = Communications and Operations Management			QA7 = Systems Acquisition, Development, and Maintenance			QA8 = Incident Management			Desirability
	Aw	Tn	E	SoD	CM	NS	SoA1	SoA2	SoAn	P1	P2	Pn	
1	0.9524			0.8333			1.0000			1.0000			89.27%
2	0.9524			0.8333			0.0025			1.0000			40.60%
3	0.9524			1.0000			1.0000			0.8333			42.78%
4	0.4762			0.8333			1.0000			0.8333			73.32%
5	0.4762			0.8333			0.8333			1.0000			35.94%
6	0.0014			1.0000			1.0000			1.0000			44.75%
7	0.9524			0.8333			1.0000			0.8333			43.85%
8	0.4762			0.8333			1.0000			1.0000			81.58%
9	0.4762			0.8333			1.0000			1.0000			33.95%
10	0.4762			0.0025			0.8333			1.0000			36.13%

As evidenced, each SCC has been evaluated using the identified features for each quality attribute. The binary input scale is used to determine the presence of features. Using the proposed approach, the most desirable SCC (based on Table 3) is SCC 1 (highest Desirability), followed by SCC 8, SCC 4, and so on. It is important to notice that the evaluation of SCC using this approach is fully dependent on the particular scenario at hand. In this case assessment, the results are based on the parameters configured in Table 2. However, if changed to reflect more priority on different quality attributes, the results would vary from the ones presented in Table 3. In addition, different applications of the approach can contain numerous features, which make it fully customizable for practical applications.

CONCLUSION, CONTRIBUTIONS, AND FUTURE RESEARCH

The research presented in this paper develops an innovative approach for evaluating the quality of SCC in organizations based on a multiple quality evaluation criteria. Specifically, it presents a methodology that uses Desirability Functions to create a unified measurement that represents how well SCC meet quality attributes and how important the quality attributes are for the organization. Through a case assessment, the approach is proven successful in providing a way for measuring the quality of SCC for specific organizations.

There are several important contributions from this research. First, the approach is simple and readily available for implementation using a spreadsheet. This can promote usage in practical scenarios, where highly complex methodologies for SCC selection are impractical. Second, the approach fuses multiple evaluation criteria and features to provide a holistic view of the overall SCC quality. Third, the approach is easily extended to include additional quality attributes not considered within this research. Finally, the approach provides a mechanism to evaluate the quality of SCC in various domains. By modifying the parameters of the Desirability Functions, quality of SCC can be evaluated by considering only the quality attributes that are necessary for the organization. Overall, the approach presented in this research proved to be a feasible technique for organizations to effectively and efficiently evaluate the quality of SCC over their financial information.

Regarding future research work, criteria factors (targeting other specific organizations' restrictions, goals, regulations, etc.) can be added to improve the current investigation. In addition, experts from similar industries or organizations may be interviewed to identify a more accurate set of evaluation criteria that can potentially be utilized as guidelines, policies, or procedures for the organization under evaluation. To extend the research, results from this paper can be examined and compared to SCC assessment results from other similar organizations. A further opportunity would utilize a hybrid approach (i.e., Desirability Functions combined with other traditional methodologies) to assess SCC. A hybrid approach can certainly strengthen current SCC evaluation processes in organizations.

REFERENCES

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

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

Cooke, I. (2019). Auditing Cybersecurity. *ISACA Journal volume 2*, 2019. Retrieved September 1, 2019, from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/is-audit-basics-auditing-cybersecurity

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

Deloitte’s Risk Advisory (November 2018). General IT Controls (GITC) Risk and Impact. Retrieved October 15, 2019, from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-general-it-controls-noexp.pdf

Derringer, G., & Suich, R. (1980). Simultaneous optimization of several response variables. *Journal of Quality Technology*, *12*(1), 214-219.

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. *Appeared in International Conference on Security and Management*, July 16-19.

Federal Bureau of Investigation's (FBI). (2019). *White-Collar Crime*. FBI Major Threats & Programs – What We Investigate. Retrieved September 1, 2019, from 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. http://dx.doi.org/10.1016/j.cose.2008.07.009.

Global Technology Audit Guide (GTAG) 2: *Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition.* The Institute of Internal Auditors. (2012). Retrieved April 3, 2019, from https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx

Global Technology Audit Guide (GTAG) 8: *Auditing Application Controls*. The Institute of Internal Auditors. (2009). Retrieved April 3, 2019, from https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx

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.

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

ISACA. (2009). COBIT and Application Controls: A Management Guide. Retrieved September 1, 2019, from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-and-Application-Controls-A-Management-Guide.aspx

ISACA. (2011). Web Application Security: Business and Risk Considerations. Retrieved September 1, 2019, from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Web-Application-Security-Business-and-Risk-Considerations.aspx

Information Technology Infrastructure Library (ITIL) Change Management. (2016). BMC Software, Inc. Retrieved September 1, 2019, from www.bmc.com/guides/itil-change-management.html

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. Retrieved October 10, 2019, from https://www.isaca.org/Journal/archives/2019/Volume-2/Pages/why-security-product-investments-are-not-working.aspx

Krishnan, G. V., & Visvanathan, G. (2007). Reporting Internal Control Deficiencies in the Post-Sarbanes-Oxley Era: The Role of Auditors and Corporate Governance. *International Journal of Auditing, 11*(2), 73-90.

Lavion, D. (2018). *Pulling fraud out of the shadows*. Global Economic Crime and Fraud Survey 2018. PricewaterhouseCoopers LLP. Retrieved September 1, 2019, from https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html#cta-1

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

Masli, A., Richardson, V.J., Watson, M.W., & Zmud, R.W. (2016). Senior Executives' IT Management Responsibilities: Serious IT-Related Deficiencies and CEO/CFO Turnover. *MIS Quarterly, 40*(1), 687-708.

Mitra, P., & Mishra, S. (2016). Behavioral aspects of ERP implementation: A conceptual review. *Interdisciplinary Journal of Information, Knowledge, and Management, 11*(1), 17-30.

Montgomery, D. (2008). *Design and analysis of experiments, 7th Edition*. New York, NY: John Wiley & Sons, Inc.

Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). *How to Increase Awareness*. ISACA Journal volume 2, 2019. Retrieved September 1, 2019, from http://www.isacajournal-digital.org/isacajournal/2019_volume_2/MobilePagedArticle.action?articleId=1468061#articleId1468061

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. DOI: 10.33642/ijbass.v5n6p4

Otero, A. R. (2019b). System Change Controls: A Prioritization Approach Using Analytic Hierarchy Process. *International Journal of Business and Applied Social Science, 5*(8), 34-46. DOI: 10.33642/ijbass.v5n8p4

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

Otero, A. R. (2015a). An Information Security Control Assessment Methodology for Organizations' Financial Information. *International Journal of Accounting Information Systems, 18*(1), 26-45. DOI: 10.1016/j.accinf.2015.06.001

Otero, A. R. (2015b). Impact of IT Auditors' Involvement in Financial Audits. *International Journal of Research in Business and Technology, 6*(3), 841-849. DOI: 10.17722/ijrbt.v6i3.404

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. DOI: 10.4018/jdtis.2011070103

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 Applications, 2*(4), 1-11. DOI: 10.5121/ijnsa.2010.2401

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. DOI: 10.5121/ijnsa.2019.11601

Otero, A. R., Tejay, G., Otero, L. D., & Ruiz, A. (2012). A Fuzzy Logic-based Information Security Control Assessment for Organizations. *Appeared in IEEE Conference on Open Systems*, October 21-24 at Grand Seasons Hotel, Kuala Lumpur, Malaysia. DOI: 10.1109/ICOS.2012.6417640

Pillai, A. K. R., Pundir, A. K., & Ganapathy, L. (2014). Improving Information Technology Infrastructure Library Service Delivery Using an Integrated Lean Six Sigma Framework: A Case Study in a Software Application Support Scenario. *Journal of Software Engineering and Applications, 7*(1), 483-497. http://dx.doi.org/10.4236/jsea.2014.76045

Post, G. V., & 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. Retrieved October 14, 2019, from https://www.pwc.at/de/publikationen/global-economic-crime-survey-2014.pdf

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

Schwartz, M. (1990). Computer security: Planning to protect corporate assets. *Journal of Business Strategy, 11*(1), 38-41.

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.

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.

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.

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.