QUALITY ASSESSMENT OF ACCESS SECURITY CONTROLS OVER FINANCIAL INFORMATION

Angel R. Otero, Christian Sonnenberg and LuAnn Bean

Nathan M. Bisk College of Business, Florida Institute of Technology, Melbourne, Florida, USA

ABSTRACT

Information security necessitates the implementation of safeguards to guarantee an adequate defense against attacks, threats, and breaches from occurring. Nonetheless, even with "adequate" defensive efforts, the taste for accessing sensitive and confidential financial information is too tempting, and attacks continue to escalate. Organizations must plan ahead so that identified attacks, threats, and breaches are appropriately managed to a successful resolution. A proven method to address information security problems is achieved through the effective implementation of access security controls. This paper proposes a quantitative approach for organizations to evaluate access security controls over financial information using Analytic Hierarchy Process (AHP), and determines which controls best suit management's goals and objectives. Through a case study, the approach is proven successful in providing a way for measuring the quality of access security controls over financial information based on multiple application-specific criteria.

KEYWORDS

Information Security, Access Security Controls, Internal Controls, Analytic Hierarchy Process, Pairwise Comparisons.

1. INTRODUCTION

Information security has been referred to as the practices, techniques, and/or tools put in place to protect information confidentiality, integrity, and availability [1]. It prompts for the implementation of multiple layers of safeguards in order to guarantee an adequate defense against attacks, threats, and breaches. However, even with "adequate" defensive mechanisms, the sensitive nature of financial information is too tempting, and attacks like cybercrime, threats, and breaches continue to escalate [1], [2]. Figure 1 provides statistics on the U.S. states with the largest cybercrime losses reported in 2018 [42].

DOI: 10.5121/ijnsa.2019.11601

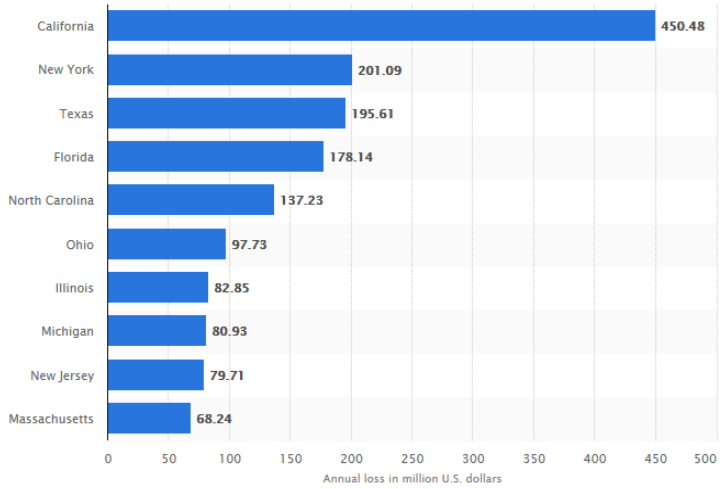

Figure 1. Cybercrime losses by state reported in the U.S. in 2018 (in million U.S. dollars)

As [3] points out, examples of sensitive financial information include transactions related to the areas of globalization, intercompany trades, and mergers and acquisitions. These transactions create risks related to financial and regulatory reporting. It is no surprise that since the introduction of the Sarbanes-Oxley Act of 2002 (SOX), improving efficiency of business processes has become a top priority for senior management. According to a 2016 survey conducted by the SOX & Internal Controls Professionals Group (a group of 3,000 plus members), improving the efficiency of the SOX function was identified as a top priority, followed by ensuring compliance with SOX and other laws and regulations [4]. Increasing the focus on cyber and information technology (IT) controls was also shown as a top priority in the survey [4].

Improving effectiveness and efficiency of business processes also includes the safeguarding of organization software hosting business information. Figure 2 shows primary attack points for data breaches in the U.S. as of 2018, evidencing software as the primary attack point [43]. According to [5] and [6], the absence of controls or the implementation of weak controls opens up opportunities for this type of fraud risk. Corporate fraud (or white-collar crime), based on [7], is among the Federal Bureau of Investigation's (FBI) highest criminal priorities. Corporate fraud translates into significant losses for companies and their investors, and continues to cause immeasurable damage to the U.S. economy. The majority of the corporate fraud identified by the FBI involves fraudulent trades; false accounting entries; data manipulation; misrepresentations of financial condition; and/or illicit transactions to evade regulatory oversight [7]. A 2014 Global Economic Crime Survey performed by PricewaterhouseCoopers LLP [8] studied the views of over 5,000 participants from more than 100 countries regarding the frequency and direction of corporate fraud. The survey revealed that over half of U.S. participants reported their companies experienced fraud or inconsistencies with their financial systems in excess of $100,000 while 8% reported fraud in excess of $5 million. Furthermore, web applications are susceptible to many security risks and vulnerabilities dealing with financial information, thus creating significant exposure for many organizations [9], [10]. Based on a 2017 study made by the American Accounting Association, organizations with weak entity-level controls (i.e., material weaknesses) were 90% or more prone to have fraud versus organizations with established strong controls [11]. The need for strong controls is forcing organizations to invest more time revaluating risks and, most importantly, identifying controls that are effective and efficient to ensure the prevention of

fraud and safeguarding information. The facts just presented paint a troubling picture and serve as an incentive for identifying novel ways to assist organizations in the enhancement of processes to secure, manage, and control valuable information.

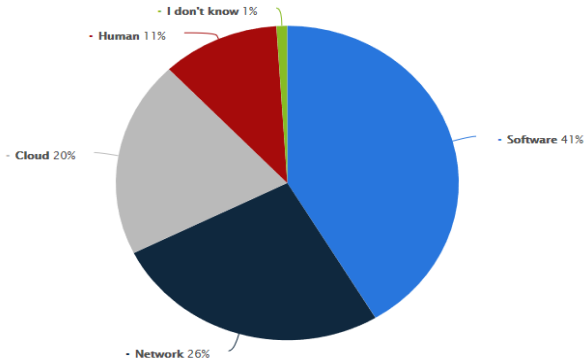

Figure 2. Primary attack points for data breaches in the U.S. as of 2018

In today's organizational culture, most information security challenges are addressed with security tools and technologies such as encryption, firewalls, access management, etc. [12], [13], [14]. Although tools and technologies are an integral part of organizations' information security plans, it is argued that they alone are not sufficient to address information security problems [15], [16], [17]. Organizations must plan ahead so that identified attacks, threats, and breaches can be appropriately managed with timely and successful resolutions.

A proven method to address the security problem is through the effective implementation of access security controls (ASC) [18]. Organizations must thoroughly evaluate and select appropriate ASC that satisfy their specific security requirements [19], [20], [21]. However, due to a variety of organizational-specific constraints (e.g., cost, availability of resources, scheduling requirements, etc.), organizations do not have the luxury of implementing all required ASC. Evaluations of ASC may thus be necessary to ensure adequate selection (and further implementation), taking into account organizational business constraints.

According to literature, traditional ASC evaluation methodologies used in organizations do not necessarily promote an effective assessment, prioritization, and implementation of such controls. For instance, the selection of ASC in organizations based on traditional methods has mostly been determined using yes or no type answers (e.g., whether the control is relevant or not, etc.). The problem here is that imprecision (i.e., degree of relevance or significance for each ASC) is not being considered. This illustrates a major problem that can impact the security of critical financial information. An accurate and complete evaluation of ASC must address and measure how relevant ASC are prior to their selection.

This paper proposes a quantitative approach to assist management in evaluating and ultimately selecting ASC. The proposed approach uses Analytic Hierarchy Process (AHP), a multi-attribute decision-making method, to determine which ASC best suit management's goals and needs based on specific quality criteria. This provides management with a measurement that can be used as the main metric for selecting ASC. The remainder of the paper is organized as follows. Section 2 provides a summary of previous work on ASC selection. Section 3 describes the proposed solution approach. Section 4 provides detailed explanations of the AHP method. Section 5

presents the evaluation and results of a case study, while Section 6 shows summarized conclusions and contributions of the proposed approach. Lastly, Section 7 provides limitations and future work.

2. BACKGROUND WORK

According to [19], the process of identifying effective ASC in organizations has been a challenge in the past, and numerous attempts have been made to come up with the most effective way possible. For instance, risk analysis and management (RAM) has been recognized in the literature as an effective approach to identify ASC [19]. RAM consists of performing business analyses to determine information security requirements [19]. An ASC is then put into place to mitigate the risks resulting from the analyses performed. RAM, however, has been described as a subjective, bottom-up approach [22], not necessarily taking into account unique organizational constraints.

The use of best practice frameworks is another approach widely used by organizations to introduce minimum controls in organizations [19]. The author in [23] states that best practice frameworks assist organizations in identifying appropriate ASC. Some best practices include Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE). The researchers in [20] mentioned other best practice frameworks, which also assist in the identification and selection of ASC. These are: International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 177995, 27001, and 27002; PROTECT, Capability Maturity Model (CMM), and Information Security Architecture (ISA).

The process of selecting effective ASC from best practice frameworks, however, is not a straight forward one [22]. The authors in [22] state that best practice frameworks leave the identification and selection of controls to the user. Because of that, they offer minimum guidance in determining the best controls to safeguard a particular business situation. Frameworks do not always take into consideration organization-specific constraints (e.g., costs of implementation, scheduling requirements, resource constraints, etc.). Other informal methods used include ad hoc or random approaches, which could lead to the inclusion of unnecessary controls and/or exclusion of required controls [19].

In a different study, a legal requirements determination model was developed for defining and recommending legal requirements and relevant controls, respectively [24]. Legal information security requirements resulted from a legal compliance questionnaire combined with a matrix that mapped legal aspects within each of the proposed legal categories to all related ISO/IEC 27002 controls. Following determination of the legal requirements, a list of relevant controls from the ISO/IEC 27002 framework, including ASC, was produced to satisfy the previously identified legal requirements. The structure model developed by [24]: assisted in establishing information security requirements from a legal perspective; provided an interpretation of the legal source associated with information security requirements; and proposed potential controls from the ISO/IEC 27002 best practice framework to address the already identified legal information security requirements. Nonetheless, as evidenced earlier, the selection of controls from best practice frameworks is not adequate as they offer minimum guidance in determining effective controls for a particular organization [22].

In [25], an innovative control evaluation and selection approach was developed to help decision-makers in resource-constrained environments select the most effective information security controls (ISC). The approach used desirability functions to quantify the desirability of each ISC after taking into account the benefits and restrictions associated with implementing the particular control. The above provided management with a measurement that was representative of the overall quality of each ISC based on organizational goals. Through a case study, the approach proved successful in providing a way for measuring the quality of ISC in organizations. The methodology in [25] took into consideration relevant quality attributes of each ISC in order to determine their relative importance. The attributes were defined as different features, where each feature was determined by the organization to either be present or not. Once all features were identified, each individual ISC was evaluated against each feature using a simple binary or boolean scale (0 or 1). The ISC that satisfied the highest number of features exposed a higher level of quality (or desirability) for that particular quality attribute. The above resulted in a control evaluation approach, based on how well ISC met quality attributes, and how important those quality attributes were for the organization. However, a binary or boolean criteria for evaluating quality attributes may not be a precise enough assessment for selecting ISC.

Checklists are another very common method used in organizations to identify and select ASC. The authors in [26] used checklists as a framework to identify common ASC, including information security risks within cloud-based organizations. Numerous information security checklists have been proposed and used over the years [27]. Their significance, according to [28], has been on identifying "all possible threats to a computer system and propose solutions that would help in overcoming the threat" (p. 294). However, according to [28], the use of checklists has declined over time simply because they "provide little by way of analytical stability" (p. 294). Even though checklists may be viewed as good means to ensure information security, exclusive reliance on them could result in a flawed information systems security strategy [28]. Furthermore, [29] argue that although checklists draw concern on particular procedures, they do not thoroughly address the key task of understanding the substantive questions. Checklists are basically concerned with what can be done without any analytical stability in regards to the kind of actions identified [27].

In [18], a methodology was developed to address weaknesses in the existing literature pertaining to the evaluation of ISC in organizations' financial systems. The methodology used fuzzy set theory to allow for a more accurate assessment of imprecise criteria (compared to traditional methodologies) which, in turn, resulted in a more effective selection of ISC and enhanced information security in organizations [18], [45]. Overall, the developed methodology proved to be a feasible technique for evaluating ISC in organizational financial systems. Due to convenience and availability, the research performed by [18] involved a single university located in the southeast U.S. within the schools, universities, and non-profit industry. Further similar studies must be performed at organizations in other locations, or from different sizes and industry types in order to generalize the findings in a broader scope. Also, implementation of the design-science research (DSR) method used to develop the methodology, represents a limitation given the rapid advances in technology that can potentially upset its results before they are implemented successfully in organizations, or before benefits can be obtained [30].

In [31], an Operational, Public image, Legal (OPL) method was proposed, using DSR, to classify the security criticality of the organization's data along three dimensions (i.e., operations, public image, and firm's legal/compliance exposure). Through empirical study, the authors demonstrated how the OPL method allowed for quantitative estimation of the significance of existing ISC, as

well as the risk of missing controls. In other words, the model was designed to guide strategies for testing in-place ISC, as well as for determining which ISC may need to be incrementally added. Questionnaires were completed by senior information security officers and internal auditors supporting the developed model, and its acceptability and usefulness in the organization. Nonetheless, as stated by [28], the significance of information security checklists or questionnaires has declined simply "because they provide little by way of analytical stability" (p. 294). Furthermore, [29] argued that although checklists or questionnaires draw concern on particular details of procedures, they do not completely address the key task of understanding the substantive questions. Checklists and/or questionnaires are concerned about what can be done without any analytical stability in regards to the kind of actions identified [27].

Another research study from [32] developed an information security control prioritization (ISCP) model to determine critical ISC consistent with an assessment criterion. The model used techniques from the Order Performance by Similarity to Ideal Solution (TOPSIS) method (a sub-method of multiple attribute decision making). Assessment of ISC using TOPSIS involved a multi- and dynamic evaluation model that assists organizations in evaluating ISC accurately. The model enabled adequate security decision making by considering assigned weights of each assessment criterion within the organization. With management-assigned weights, the TOPSIS model helped the organization identify and implement only the most effective and critical ISC. Nevertheless, significant decision making based strictly on management's assigned weights (subjective in nature) may not necessarily be the most objective, nor considered a precise enough assessment for selecting ISC in organizations.

The authors in [33] developed an automated decision support system to assist in the identification of security controls for a particular system and context (i.e., banking domain). The developed system was based on machine learning, and leveraged historical data from security assessments performed over past banking systems. The authors operationalized and empirically evaluated their developed system using real historical data from the banking domain in order to recommend security controls. Results suggested that the system provided effective decision support for security controls. Evaluation metrics for the developed system were limited in scope to security controls for which there were at least five occurrences in the historical data. Below this threshold of five events, applying machine learning according to the authors was not meaningful. Generalizability of results represented another limitation and important concern of the research. While the historical information drawn for system development purposes was consistent with commonly used and well-known ISO standards, additional case studies are needed for assessing and validating whether the developed system remains effective in other application contexts. Particularly, to ensure and support the accuracy and relevance of the automated selection process, further investigations are necessary along with a more longitudinal study.

Table 1 summarizes the differences and weaknesses from the above approaches and methodologies used in organizations to assess ASC. As seen, it is a critical task for organizations to select the most appropriate security control or ASC in order to safeguard their information. As a result, new methods to select ASC must be developed that are not only effective and efficient, but also consider constraints and restrictions that are unique to the organization.

Table 1. Literature-based weaknesses in ASC assessment methodologies.

ASC Assessment Approach	Literature-based Weakness(es)
Risk Analysis and Management (RAM) [19], [22] Legal Requirements Determination Model [24], [22]	- Subjective, bottom-up approach that does not consider specific organizations' constraints. - Selected controls may be unnecessary or relate to trivial issues.
Best Practice Frameworks [19], [23], [20]	- Leave the identification of ASC to the user, while offering little guidance in determining the best ASC to provide adequate security for the particular business situation. - Do not necessarily account for organization specific constraints.
Ad Hoc or Random Approaches [19], [23]	- Lead to the inclusion of unnecessary ASC and/or exclusion of required ASC.
Desirability Functions [25]	- A binary or boolean criteria for evaluating the quality attributes of ASC is not considered a precise enough assessment for selecting ASC in organizations.
Information Security Checklists [26], [27], [28], [29] Operational, Public image, Legal (OPL) Method [31], [28], [29], [27]	- Provide little by way of analytical stability. - Exclusive reliance could result in a flawed information security strategy. - Do not completely address the key task of understanding the substantive questions. - Concerned on what can be done without any analytical stability regarding the kind of actions identified.
DSR-based Methodology [18], [30]	- Given rapid advances in technology, DSR results can be outrun by technology before they even show up in the literature.
TOPSIS-based Information Security Control Prioritization Model [32]	- Subjective in nature; not considered a precise enough assessment for selecting ASC in organizations.
Machine Learning-based Automated Decision Support System [33]	- Limited ASC evaluation based only on historical data, risking results' meaning and relevance. - Generalizability concern; additional, more longitudinal assessment studies are needed for validation, accuracy, and relevance.

3. SOLUTION APPROACH

To properly evaluate the quality and significance of ASC in organizations, management must follow a methodology that only takes into consideration relevant attributes of the ASC. Such methodology must allow management to compare how well ASC perform based on predefined evaluation criteria in order to determine the relative significance of each ASC. The methodology must also allow management to assign priorities to the evaluation criteria to customize the results based specifically on organizational needs. To achieve this, the AHP-based methodology created

in [34] is modified and customized to solve the problem of prioritizing ASC in organizations. In [34], the authors presented a user-centric and application-specific quality of service (QoS) assessment methodology for cellular communication networks. Specifically, the authors used AHP to create a unified measurement that represents how well cellular networks' services were perceived given particular sets of application classes and relative to other networks servicing in the same area. The methodology was based on the data collected through drive testing and focused on data services. Through multiple case studies, the approach was proven successful in providing a way for analyzing user-centric QoS for application-specific scenarios.

In a different, but more recent research study, [35] used fuzzy AHP to prioritize and select effective managerial domains and control objectives in information security controls. This research focused on the process of implementing ISO 27001 information security areas in the National Iranian Oil Products Distribution Company. According to results, the area of access controls, as well as the area of information systems acquisition, development, and maintenance both resulted in the highest priorities among the information security controls for managerial domains. Other ISO 27001 information security areas such as business continuity management and asset management resulted in the lowest priorities among the assessed security-related controls. Moreover, the research found that among 39 information security control objectives, user access management, and third-party service delivery management objectives had the highest and lowest priorities, respectively.

For this particular research, the proposed AHP methodology will compare multiple ASC 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 ASC. The output provided can be used as a unified measurement of the ASC as perceived by management.

4. ANALYTICAL HIERARCHY PROCESS

AHP is a multi-attribute, decision-making method used to facilitate decisions that involve multiple competing goals [36]. According to [46], AHP is one of the most significant and effective multicriteria decision-making methods in use. AHP was first introduced by [47] to solve unstructured problems in the fields of economics, social, and management sciences, and it has been applied ever since in practical scenarios in many other fields. AHP allows decision-makers to structure complex problems using hierarchies that systematically assess quantitative and qualitative factors based on multiple application-specific criteria [48]. Once the factors have been assessed against the specified criteria, decision-makers select the best alternative or the alternative with the highest weight.

AHP provides a powerful tool that can be used to assess different ASC 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 may include 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 could 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 ASC is presented in Figure 3.

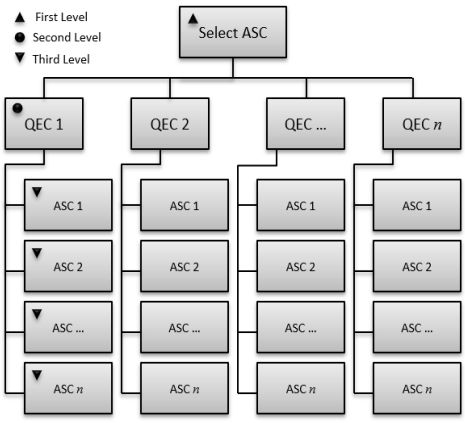

Figure 3. AHP hierarchy for ASC evaluation

The second and third levels of the AHP hierarchy vary according to the ASC available and the QEC selected for evaluating the ASC. The second level can be extended to include other QEC, such as: the required number of systems the ASC should provide security to (i.e., scope); which organization objectives must be met by the ASC; and which physical access locations are to be protected by the ASC. The third level consists of the actual ASC being evaluated. For purposes of this paper, three ASC were considered, ASC1, ASC2, and ASC3. In other scenarios, there could be n ASC, each providing different measurements for each QEC identified. Once the hierarchy is built, and relevant QEC measurements taken for each ASC, a common scale is created to rank each ASC. That is, for each comparison made during the AHP, a common, pair-wise comparison scale is used to determine how preferred one option is over another. This allows standardization in all comparisons made during the AHP process. Table 2 presents the pairwise comparison scale created for the quality evaluation problem.

Table 2. 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

Quality evaluators establish preferences between different ASC using the pairwise comparison scale and pairwise comparison matrices [36]. There are two types of pairwise comparison matrices in AHP, the ASC vs. ASC matrices, and the QEC vs. QEC matrix. The ASC vs. ASC pairwise comparison matrices are n x n matrices where each element aij represents how much more desirable the ASC at row i is than the ASC at column j in terms of a pre-defined QEC. The format of the ASC vs. ASC matrices is presented in (1), where Az is the pairwise comparison matrix for QEC z (i.e., z $\in$ {restrictions, access security, human resources}) and I_x represents ASC 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 ASC in the pairwise comparison matrix. That is, assuming weight vector W = [w_1 w_2 … w_n], the value of w_i represents the relative importance of ASC 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 Az 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 ASC vs. ASC 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 x 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 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 ASC vs. ASC matrices. Once all weight vectors in the quality evaluation problem have been computed, they are used to determine the ASC that provides the best quality. For example, assuming a quality evaluation problem with x number of QEC and y number of ASC, the AHP provides y+1 weight vectors; one (W_A) associated with the QEC vs.

QEC pairwise comparison matrix, and the rest W_i associated with each ASC versus ASC matrix i, as illustrated in Figure 4.

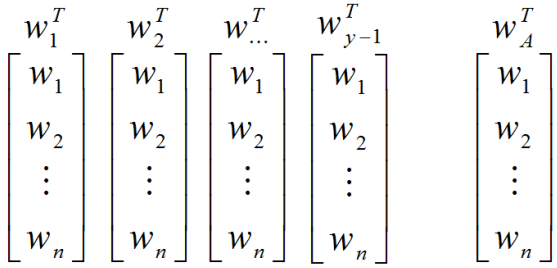

Figure 4. AHP weight vectors

Figure 4. AHP weight To compute the relative preference for ASC i, we let W = W_i, WA = W_A, and define Si as the overall score for ASC i, then,

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

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

5. CASE STUDY EVALUATION AND RESULTS

This section presents the results of a quality evaluation case study using the proposed approach. The case study evaluates the quality of any three ASC in organizations (i.e., ASC1, ASC2, and ASC3). The types of QEC depend on the particular criteria being evaluated. For this case study, the QEC below were used by [25] and include restrictions, access security, and human resources [37], [38], [39], [40], [41], [44]. These criteria are described below:

1. Restrictions – There are restrictions that management must take into account before selecting ASC. Some of these may include whether the costs involved in the selection and implementation of the ASC are considered high by the organization, whether resources are not available, and whether there are scheduling constraints associated with implementing the ASC.

2. Access Security – Implementation of an ASC will promote appropriate levels of access security to ensure the protection of the organization's systems and applications against unauthorized activities. Organizations may implement network access controls, operating systems access controls, and application controls based on their specific needs.

3. Human Resources – Implementation of human resources access controls supports reductions of risk of theft, fraud, or misuse of computer resources by promoting information security awareness, training, and education for employees. Depending on the particular situation,

costs, and the availability of personnel, organizations may select which of these human resources controls to employ.

To evaluate the quality provided by the ASC, pairwise comparisons of each ASC in terms of each QEC are performed. Each ASC is compared using the comparison scale specified in Table 2. Results are presented below in Tables 3, 4, and 5.

Table 3. ASC vs. ASC comparison matrix, normalized matrix, and weight vector for QEC Restrictions.

Restrictions	**ASC1**	**ASC2**	**ASC3**
ASC1	1	4	3
ASC2	0.25	1	0.33
ASC3	0.33	3	1
Total	1.58	8	4.33

Restrictions	**ASC1**	**ASC2**	**ASC3**	**Total**
ASC1	0.63	0.50	0.69	1.82
ASC2	0.16	0.13	0.08	0.37
ASC3	0.21	0.38	0.23	0.82

Restrictions	**ASC1**	**ASC2**	**ASC3**
Weight	0.61	0.12	0.27

Table 4. ASC vs. ASC comparison matrix, normalized matrix, and weight vector for QEC Access Security.

Access Security	**ASC1**	**ASC2**	**ASC3**
ASC1	1	4	0.25
ASC2	0.25	1	0.20
ASC3	4	5	1
Total	5.25	10	1.45

Access Security	**ASC1**	**ASC2**	**ASC3**	**Total**
ASC1	0.19	0.40	0.17	0.76
ASC2	0.05	0.10	0.14	0.29
ASC3	0.76	0.50	0.69	1.95

Access Security	**ASC1**	**ASC2**	**ASC3**
Weight	0.25	0.10	0.65

Table 5. ASC vs. ASC comparison matrix, normalized matrix, and weight vector for QEC Human Resources.

Human Resources	**ASC1**	**ASC2**	**ASC3**
ASC1	1	0.33	0.20
ASC2	3	1	0.25
ASC3	5	4	1
Total	9	5.33	1.45

Human Resources	**ASC1**	**ASC2**	**ASC3**	**Total**
ASC1	0.11	0.06	0.14	0.31
ASC2	0.33	0.19	0.17	0.69
ASC3	0.56	0.75	0.69	2.00

Human Resources	ASC1	ASC2	ASC3
Weight	0.10	0.23	0.67

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

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 6.

Table 6. 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	0.2	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

Finally, using (5), the results of Tables 3 through 6 are combined to provide the final quality measurement for each ASC evaluated. The final quality measurement is presented in Table 7.

Table 7. ASC final quality measurement.

ASC	Quality
ASC1	47.00%
ASC2	12.42%
ASC3	40.57%

As shown, the final quality measurement shows ASC1 (47.00%) as the best performer, followed by ASC3 (40.57%) and ASC2 (12.42%). It is important to note that the evaluation of ASC using this approach is fully dependent on the particular organization and its specific information security objectives.

Contrary to other approaches and methodologies found in the literature to evaluate ASC (refer to Section 2), the quantitative approach developed herein strengthens information security by identifying and implementing the best defensive controls (based strictly on quality and relevance to the particular organization) against attacks, threats, and breaches. Other highlights of the developed approach include fusing unlimited quality evaluation criteria to provide a holistic view of the experienced quality, allowing the approach to be easily extended with additional quality criteria not considered within this research.

6. CONCLUSIONS AND CONTRIBUTIONS

The research presented in this paper develops an innovative approach for evaluating the quality of ASC in organizations based on multiple quality evaluation criteria. Specifically, the paper proposes a quantitative approach for organizations to evaluate ASC over financial information using AHP to determine the best controls to achieve management's goals and objectives. The AHP-based approach creates a unified measurement that represents how well ASC meet quality attributes and how important the quality attributes are for the organization. In this case study, for instance, the final perceived quality result, measured quantitatively and shown in Table 7, allows management to make a better selection of ASC. Through the case study, the proposed approach is proven successful in providing a way for measuring and evaluating the quality of ASC over organizations' financial information based on multiple application-specific criteria.

There are several important contributions from this research. First, the proposed approach is readily available for implementation using a spreadsheet. Second, it can promote usage in practical scenarios where highly complex methodologies for quality evaluation are impractical. Finally, the approach provides a mechanism to evaluate quality based on specific scenarios. By modifying the parameters of the QEC vs. QEC comparison matrix, quality can be evaluated taking into consideration many different scenarios. Overall, the approach presented in this research proved to be a feasible technique for effectively evaluating the quality of ASC in organizations.

7. LIMITATIONS AND FUTURE WORK

The authors understand and realize the benefits of testing the developed approach in a real-world setting environment. Only after implementations in a real-world setting the true benefits and/or limitations of the proposed approach will be exhibited. However, as evidenced in the literature review presented in Section 2, it is not uncommon for controls related to information security to be assessed and tested using case studies, as opposed to real-world setting scenarios. In this research, a case study was used to validate how the proposed approach would be well-suited in most organizational settings. The developed approach proved successful in providing a way for measuring the quality of ASC over financial information.

An opportunity to expand the current research involves adding criteria factors to evaluate ASC other than the ones included in this paper. Either refinement or incorporation of additional assessment factors, specifically targeting organizations' restrictions, goals, regulations, etc., can improve the current investigation. Another research opportunity would be to examine results from this paper and compare them to assessment results from other similar organizations. A further opportunity to expand the research conducted herein may be to utilize a hybrid approach (i.e., AHP combined with traditional methodologies) to assess ASC. A hybrid approach would likely strengthen current ASC evaluation processes in organizations.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers whose constructive critique greatly improved the quality of the paper.

REFERENCES

[1] Hare, S. (2019). Security Breaches: Are You Ready? Strategic Finance, [online] Available at: https://sfmagazine.com/post-entry/april-2019-security-breaches-are-you-ready/ [Accessed 5 June 2019].

[2] Otero, A. R. (2019). System change controls: A prioritization approach using Analytic Hierarchy Process. International Journal of Business and Applied Social Science, 5(8), 34-46.

[3] Tucker, I. (2018). Getting a Better Handle on Compliance and Controls. Strategic Finance, [online] Available at: https://sfmagazine.com/post-entry/december-2018-getting-a-better-handle-on-compliance-and-controls/ [Accessed 5 June 2019].

[4] SOX & Internal Controls Professionals Group. (2016). 2016 State of the SOX/Internal Controls Market Survey. [pdf] Available at: https://www.soxprofessionalsgroup.org/sites/soxpro/files/State_of_the_SOX_Market_Survey-k12214-20160906c-web.pdf [Accessed 1 June 2019].

[5] Lavion, D. (2018). Pulling fraud out of the shadows. Global Economic Crime and Fraud Survey 2018. PricewaterhouseCoopers LLP, Available at: https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html#cta-1 [Accessed 7 May 2019].

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

[7] Federal Bureau of Investigation (FBI). (2019). White-Collar Crime. FBI Major Threats & Programs – What We Investigate. Available at: www.fbi.gov/investigate/white-collar-crime [Accessed 9 April 2019].

[8] 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 7 May 2019].

[9] ISACA. (2011). Web Application Security: Business and Risk Considerations, Available at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Web-Application-Security-Business-and-Risk-Considerations.aspx [Accessed 5 May 2019].

[10] 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.

[11] Donelson, D. C., Ege, M. S., & McInnis, J. M. (2017). Internal control weaknesses and financial reporting fraud. Auditing: A Journal of Practice & Theory, 45-69. Available at: http://aaahq.org/portals/0/newsroom/intnl%20cntrl%20weakness%20and%20finan%20rpt%20fraud.pdf [Accessed 5 May 2019].

[12] 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.

[13] Volonino, L., & Robinson, S. R. (2004). Principles and practice of information security. Upper Saddle River, NJ: Pearson Prentice Hall, Inc.

[14] 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.

[15] Keef, S. (2019). Why Security Product Investments Are Not Working. ISACA Journal volume 2, 2019. Available at: https://www.isaca.org/Journal/archives/2019/Volume-2/Pages/why-security-product-investments-are-not-working.aspx [Accessed 5 May 2019].

[16] 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.

[17] 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.

[18] Otero, A. R. (2015). An Information Security Control Assessment Methodology for Organizations' Financial Information. International Journal of Accounting Information Systems, 18(1), 26-45.

[19] 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.

[20] Da Veiga, A., & Eloff, J. H., P. (2007). An information security governance framework. Information Systems Management, 24(4), 361-372.
[21] Karyda, M., Kiountouzis, E., & Kokolakis, S. (2004). Information systems security policies: A contextual perspective. Computer Security, 24(1), 246-260.
[22] Van der Haar, H., & Von Solms, R. (2003). A model for deriving information security controls attribute profiles. Computers & Security, 22(3), 233-244.
[23] Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal, 39(4), 60-66.
[24] Gerber, M., & Von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. Computers & Security, 27(5), 124-135.
[25] Otero, A. R., Otero, C. E., & Qureshi, A. (2010). A multi-criteria evaluation of information security controls using Boolean features. International Journal of Network Security & Its Applications, 2(4), 1–11. doi:10.5121/ijnsa.2010.2401.
[26] 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).
[27] Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. ACM Computing Surveys, 25(1), 375-414.
[28] Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(1), 293-314.
[29] Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. European Journal of Information Systems, 5(1), 2-9.
[30] Hevner, A.R., March, S., Park, J., Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.
[31] Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. International Journal of Accounting Information Systems, 20(1), 38-64.
[32] Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. Computers & Security, 77(1), 565-577.
[33] Bettaieb S., Shin S.Y., Sabetzadeh M., Briand L., Nou G., Garceau M. (2019) Decision Support for Security-Control Identification Using Machine Learning. In: Knauss E., Goedicke M. (eds) Requirements Engineering: Foundation for Software Quality. REFSQ 2019. Lecture Notes in Computer Science, vol 11412. Springer, Cham.
[34] 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.
[35] Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. Information Systems and e-Business Management, 15(1), 1-19. doi.org/10.1007/s10257-016-0306-y
[36] 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].
[37] Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). How to Increase Awareness. ISACA Journal volume 2, 2019. Available at: http://www.isacajournal-digital.org/isacajournal/2019_volume_2/MobilePagedArticle.action?articleId=1468061#articleId1468061 [Accessed 7 May 2019].
[38] ISACA (2009). COBIT and Application Controls: A Management Guide, Available at: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-and-Application-Controls-A-Management-Guide.aspx [Accessed 7 May 2019].
[39] 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. Paper presented at the 2012 International Conference on Security and Management. Las Vegas, NV.
[40] 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

[41] 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.

[42] IC3. (July 1, 2019). Loss through cybercrime in the United States in 2018, by victim state (in million U.S. dollars) [Graph]. In Statista. Retrieved September 19, 2019, from https://www-statista-com.portal.lib.fit.edu/statistics/234993/us-states-with-the-largest-losses-through-cybercrime/

[43] Centrify. (February 26, 2019). Primary attack points for data breaches in the United States as of 2018* [Graph]. In Statista. Retrieved September 19, 2019, from https://www-statista-com.portal.lib.fit.edu/statistics/1015959/united-states-primary-attack-points-data-breaches/

[44] Ejnioui, A., Otero, C. E., & Otero, L. D. (2013). Prioritisation of software requirements using grey relational analysis. International Journal of Computer Applications in Technology, 47(2-3), 100-109.

[45] Otero, A. R., Tejay, G., Otero, L. D., & Ruiz, A. (2012, October 21). A Fuzzy Logic-based Information Security Control Assessment for Organizations. IEEE Conference on Open Systems. Kuala Lumpur, Malaysia.

[46] Zaied, A. N. H., Grida, M. O., & Hussein, G. S. (2018). Evaluation of critical success factors for business intelligence systems using fuzzy AHP. Journal of Theoretical and Applied Information Technology, 96(19), 6406-6422.

[47] Saaty, T. L. (1980). The Analytic Hierarchy Process. McGraw-Hill, New York.

[48] Gucdemir, H. & Selim, H. (2015). Integrating multicriteria decision making and clustering for business customer segmentation. Industrial Management & Data Systems, 115(6), 1022-1040.

AUTHORS

Angel R. Otero, Ph.D., CPA, CISA, CITP, CICA, CRISC is an Assistant Professor of Accounting and Academic Chair for Accounting and Finance Online Programs for the Nathan M. Bisk College of Business at Florida Institute of Technology (FIT). Dr. Otero has over 20 years of experience in the areas of public accounting and auditing, internal control audits, information technology consulting, and information systems auditing. Before joining FIT, Dr. Otero worked at Deloitte & Touche, LLP for over 10 years and attained the position of Senior Manager. His research interests involve the areas of financial audits and internal controls; information systems auditing; accounting information systems; information security audits; and risk assessments. He has published research on the assessment of general information technology controls (GITCs) surrounding financial systems. Dr. Otero is also the author of a published university textbook in the area of information systems auditing.

Christian Sonnenberg is the Associate Dean of Online & Off-Campus Programs and an Associate Professor in Information Systems at the Nathan M. Bisk College of Business at Florida Institute of Technology. He also serves as Academic Chair for the Information Technology programs. He earned his doctorate in 2013 in Computer Science from Florida Tech with a research focus in handheld and mobile usability. Previously, Dr. Sonnenberg worked as a software engineer for Harris Corporation Government Communications Systems Division (GCSD) in Melbourne, FL. While there, he was involved in a number of areas including directional wireless networks, cellular interrogation systems, and satellite image processing applications.

LuAnn Bean, Ph.D., CPA, CIA, CFE, FCPA, CGMA. Dr. Bean is Professor of Accounting at the Nathan M. Bisk College of Business, Florida Institute of Technology, Melbourne, Florida. She has published articles in The Journal of Computer Information Systems, The CPA Journal, The Accounting Historians Journal, The Ohio CPA Journal, Internal Auditing, The Petroleum Accounting and Financial Management Journal, Thunderbird International Business Review, The Journal of Corporate Accounting and Finance, The Journal of Business and Behavioral Sciences, and other professional journals. She is active in many professional organizations, including the American Institute of CPAs, the Institute of Internal Auditors, and the Association of Certified Fraud Examiners.