2014

# An Information Security Control Assessment Methodology for Organizations

Angel Rafael Otero
*Nova Southeastern University*, rotero01@yahoo.com

# An Information Security Control Assessment Methodology for Organizations

By

Angel R. Otero

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2014

We hereby certify that this dissertation, submitted by Angel R. Otero, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Gurvirender P. Tejay, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Abdel Ejnioui, Ph.D. Date
Dissertation Committee Member

_____ _____

Peixiang Liu, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Eric S. Ackerman, Ph.D. Date
Dean, Graduate School of Computer and Information Sciences

Graduate School of Computer and Information Sciences
Nova Southeastern University

2014

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

# An Information Security Control Assessment Methodology for Organizations

By

Angel R. Otero
March 2014

In an era where use and dependence of information systems is significantly high, the threat of incidents related to information security that could jeopardize the information held by organizations is more and more serious. Alarming facts within the literature point to inadequacies in information security practices, particularly the evaluation of information security controls in organizations. Research efforts have resulted in various methodologies developed to deal with the information security controls assessment problem. A closer look at these traditional methodologies highlights various weaknesses that can prevent an effective information security controls assessment in organizations. This dissertation develops a methodology that addresses such weaknesses when evaluating information security controls in organizations. The methodology, created using the Fuzzy Logic Toolbox of MATLAB based on fuzzy theory and fuzzy logic, uses fuzzy set theory which allows for a more accurate assessment of imprecise criteria than traditional methodologies. It is argued and evidenced that evaluating information security controls using fuzzy set theory addresses existing weaknesses found in the literature for traditional evaluation methodologies and, thus, leads to a more thorough and precise assessment. This, in turn, results in a more effective selection of information security controls and enhanced information security in organizations.

The main contribution of this research to the information security literature is the development of a fuzzy set theory-based assessment methodology that provides for a thorough evaluation of ISC in organizations. The methodology just created addresses the weaknesses or limitations identified in existing information security control assessment methodologies, resulting in an enhanced information security in organizations.

The methodology can also be implemented in a spreadsheet or software tool, and promote usage in practical scenarios where highly complex methodologies for ISC selection are impractical. Moreover, the methodology fuses multiple evaluation criteria to provide a holistic view of the overall quality of information security controls, and it is easily extended to include additional evaluation criteria factor not considered within this dissertation. This is one of the most meaningful contributions from this dissertation. Finally, the methodology provides a mechanism to evaluate the quality of information security controls in various domains. Overall, the methodology presented in this dissertation proved to be a feasible technique for evaluating information security controls in organizations.

**Acknowledgments**

I start by thanking God for all of the blessings that He has poured into my life. I have been blessed with an awesome life, outstanding family, and now the opportunity to complete a doctoral dissertation.

Next, I extend my deepest gratitude to my advisor, Dr. Gurvirender Tejay. Dr. Tejay, thank you for believing in me since day one and for trusting that we can perform great work together. Thank for your continuing guidance, feedback, and support. Working with you has been a great personal and learning experience. We can now say that all the time incurred paid off! Committee members, Dr. Peixiang Liu and Dr. Abdel Ejnioui, thank you both, first, for agreeing without conditions to form part of my dissertation journey, and second for your timely and candid suggestions, all of which added significant value.

I would like to specially thank my lovely wife and best friend, Ghia M. Pieraldi, for believing in me since the day I embarked on this endeavor. Thank you for your unconditional love, continuing encouragement, and support. Thank you for all the sacrifices you went through during the past five years. I complete this dissertation today mainly because of your support and trust in me. I love you with all the strengths of my heart.

Dr. Luis Daniel Otero and Dr. Carlos Otero, my brothers. Thank you for obtaining your Ph.D.'s … you knew I was next! Thank you for being so tremendous role models, personally and professionally. Thank you for challenging me to work at the next level. I have always been very proud of you two, and am thankful to God for the blessing of being called your brother. You two inspired me to achieve this major educational level.

Angel L. Otero and Lydia E. Rivera, my parents. Wow, three doctors in the house now! To both, thanks! It is an honor and tremendous privilege to be your son. You always encouraged us three brothers to go forward, not to stay stagnant. You taught us to be responsible, to love each other, and to show commitment and dedication when embarking into the challenges of life. I thank you today, among many other reasons, for the great help and support, and for always believing that I can reach higher levels in life such as becoming a Ph.D.

I would like to dedicate this achievement to my daughter, Elizabeth M. Otero, to my son, Leonardo R. Otero, and to the other brother or sister to come. I hope that the achievement I just attained today serves as encouragement and motivation for you. Remember to always work hard without harming your neighbor. Never settle for less and condition your mindset for greatness. Be respectful, be humble, and most importantly, always put God first in your lives.

## Table of Contents

## List of Tables

### Tables

## List of Figures

### Figures

# Chapter 1

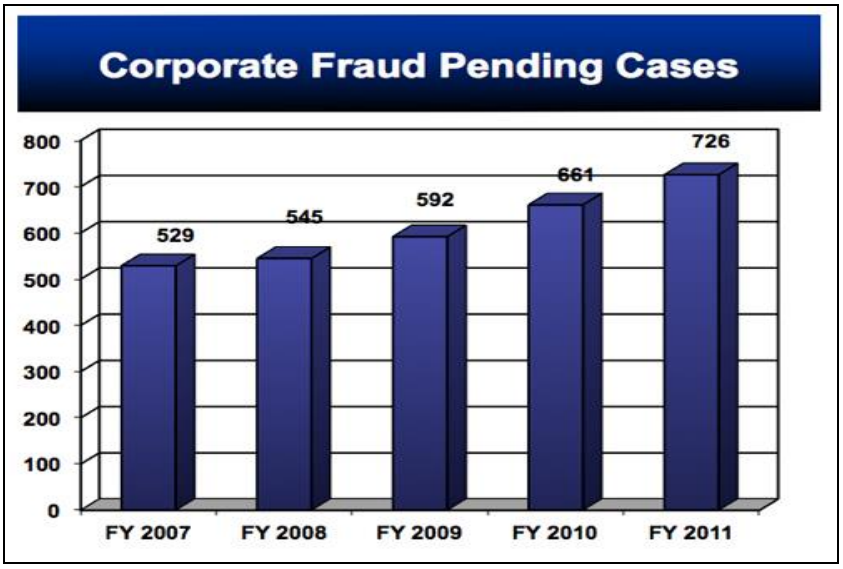
# Introduction

## 1. Background

In an era where use and dependence of computers and information systems is significantly high, the threat of incidents related to information security that could jeopardize the information held by organizations is becoming more and more serious. Throughout the years, organizations have experienced numerous losses which have had a direct impact on their information. Fraud over information is such an example. As evidenced by the Federal Bureau of Investigation (FBI), by the end of 2009, there were 592 corporate fraud cases involving manipulation and abuse of financial information throughout the United States (U.S.), several of which involved losses to public investors that individually exceeded the $1 billion mark. The FBI also reported that in 2011 alone, there were 726 pending corporate fraud cases in the U.S. involving accounting schemes designed to deceive investors, auditors, and analysts regarding the true financial condition of a corporation. Figure 1 shows the number of corporate fraud pending cases investigated by the FBI in the U.S. since 2007 through 2011.

Additionally, the 2009 CSI/FBI Computer Crime and Security Survey (conducted on 443 information security and information technology (IT) professionals in the U.S.) found that average information security losses in organizations, leading to computer security breaches, reached approximately $234,300 per respondent. Along the same line,

in a study performed by Bedard, Graham, and Jackson (2008), about 21 percent of all deficiencies detected in selected audited organizations were related to information




Note: Adapted from the Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Year, Department of Justice, U.S., 2011

**Figure 1.** U.S. corporate fraud pending cases investigated by the FBI since 2007

security. Particularly, Bedard et al.'s (2008) study noted that there were no adequate information security controls (ISC) in place within the organizations examined, and the ones in place were not operating effectively. This was the main reason for such significant percentage of deficiencies identified. To further emphasize the significance of security over organizations' information, a 2008 survey conducted by Chief Information Officer Research on 173 IT executives revealed that information security is by far the single largest potential barrier to organizations (Mather, Kumaraswamy, & Latif, 2009).

Another fact in today's organizational culture is that most information security challenges are being addressed through the use of security tools and technologies, such as, encryption, firewalls, access management, etc. (Volonino & Robinson, 2004; Vaast,

2007). 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 (Herath & Rao, 2009). To improve overall information security, organizations must evaluate (and thus implement) appropriate ISC 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., costs, availability of resources, etc.), organizations do not have the luxury of selecting and implementing all required ISC.

The alarming facts and figures just presented point to existent inadequacies and inefficiencies in regards to information security practices, while also serve as motivation for finding innovated ways to assist organizations improve their capabilities for securing valuable information. To this end, it is imperative that ISC around systems and applications in organizations be evaluated and, most importantly, accurately prioritized so that only the best and most appropriate ones get implemented. Adequate selection and implementation of ISC reduce opportunities for information system failures. Simultaneously, the effective operation of ISC assists organizations in maintaining a well-designed and controlled information systems environment.

Research efforts have resulted in various approaches and methodologies developed to deal with the ISC assessment problem. A closer look at these approaches and methodologies highlights various opportunities to create new methodologies for ISC evaluation with the potential to significantly improve the overall information security in organizations. For instance, and as will be supported in the next Chapter, there have been weaknesses identified in traditional ISC assessment methodologies that can preclude an

effective assessment and, therefore, implementation of ISC in organizations over their information.

### 1.1 Problem Statement

Adequate evaluation of ISC is crucial to organizations in maintaining sound information security as well as in protecting their information assets. Nevertheless, the literature points out several issues, gaps, weaknesses, and/or inadequacies within traditional ISC assessment methodologies that prevent an effective assessment of ISC in organizations. To mention one, the selection of ISC in organizations using traditional methods has been mainly determined based on crisp or dichotomous values (i.e., yes or no type answers based solely on decision makers' preferences). Organizations base their selection process subjectively on whether the ISC is either relevant or not. ISC that are determined to be relevant will be selected and implemented. There are other reasons that cause current ISC assessment methodologies to prompt for improvement. For example, some methodologies do not adequately account for organization constraints (e.g., costs, resource availability, scheduling of personnel, etc.), while other methodologies leave the identification of ISC to users, resulting in the potential inclusion of unnecessary ISC and/or exclusion of required ones. Furthermore, there are less formal assessment methodologies that base their ISC selection on ad hoc or random approaches, leading once again to the potential inclusion of unnecessary ISC and/or exclusion of required ISC. To continue on, ISC assessment methodologies based on checklists could result in a flawed information security strategy as checklists are concerned on what can be done without any analytical stability about the kind of actions identified. For a complete

description of weaknesses found in the literature related to ISC assessment methodologies, refer to Chapter two.

The weaknesses identified above not only affect the ISC selection process, but also impact the overall protection of the information's confidentiality, integrity, and availability (Saint-Germain, 2005). In other words, the lack of adequate information security over valuable, sensitive, or critical financial information may allow for (1) fraud, manipulation, and/or misuse of data; (2) security-related deficiencies and findings; (3) bogus trades to inflate profits or hide losses; (4) false accounting journal entries; (5) computer security breaches; and (6) false transactions to evade regulators, among others.

Traditional ISC assessment methodologies, such as, Risk Analysis and Management (RAM), baseline manuals or best practice frameworks (e.g., OCTAVE, NIST, etc.), ad-hoc approaches, and checklists, among others, must therefore be strengthened and improved to assist organizations with their ISC selection process. The existence of weaknesses within these traditional ISC assessment methodologies does not promote an effective assessment, selection, or prioritization of ISC in organizations over their information. Effective information system security implementation requires identification, assessment, and prioritization of the most appropriate ISC (van der Haar & von Solms, 2003), taking into account the issues presented above. In order to increase the effectiveness of the evaluation and selection process for ISC in organizations, new, effective, and efficient assessment methods need to be developed. Development of such assessment methodology constitutes a significant contribution to the information security literature. The aim of this dissertation or research problem was, therefore, to develop an ISC assessment methodology that adequately address the existing weaknesses identified

in traditional ISC assessment methodologies, resulting in a more effective selection of ISC and, in turn, enhanced information security in organizations.

### 1.2 Dissertation Goal

The goal of this dissertation was to develop an assessment methodology that (a) considers all-inclusive scenarios when evaluating ISC; (b) adequately accounts for organizations' restrictions and constraints; (c) significantly minimizes subjectivity and ambiguity (via providing precise evaluation values for ISC); and (d) prevents unnecessary and random ISC selections. The aforementioned methodology can better assist organizations when selecting ISC in order to mitigate information security risks.

As it will be explained and evidenced in later chapters, fuzzy set theory (FST) allows for a more adequate representation of imprecise parameters (i.e., when determining the importance of ISC) than existing and traditional methodologies. An evaluation of ISC using FST could therefore lead to a thorough, more detailed assessment by providing precise values, thus, supporting a more effective ISC evaluation and prioritization, ultimately improving information security in the organization.

### 1.3 Research Questions and Hypotheses

Currently, there are significant weaknesses in traditional ISC assessment methodologies that can prevent the effective assessment, prioritization, and implementation of ISC in organizations over their information. Failure of paying adequate attention to address these weaknesses and/or inadequacies may open up opportunities for information security breaches which can negatively impact organizations, including their IT environments. Some of these information security breaches may include security-related deficiencies and findings; false accounting journal

entries; false transactions to evade regulators; bogus trades to inflate profits or hide losses; and fraud, manipulation, and/or misuse of data; among others.

The purpose of this dissertation was to develop a methodology that corrects weaknesses identified in existing ISC assessment methodologies, and explore whether such new methodology enhance the overall information security in organizations. A methodology that resolve the weaknesses identified, while capable of modeling imprecise parameters (i.e., criteria for determining relevance) when evaluating ISC will result in a more accurate assessment, which is crucial to determine the best ISC. One technique that can be used to address the limitations stated above is through FST.

The FST-based ISC assessment methodology is expected to address the weaknesses identified in current evaluation processes by (a) contemplating all-inclusive ISC scenarios; (b) employing a less-subjective, accuracy-based method; (c) preventing / eliminating the random and unnecessary selection of ISC; (d) considering organizations' restrictions and constraints; and (e) improving, in turn, the overall information security in organizations.

To recall, the research problem described earlier was to develop a methodology that addresses the existing weaknesses in traditional ISC assessment methodologies, which may result in an enhanced information security in organizations. Consistent with the above, the research questions (RQ) to be addressed by this dissertation follow:

> RQ1: How does an ISC assessment methodology that is developed using FST address the weaknesses identified in the academic literature for traditional assessment methodologies?

RQ2: To what extent does an ISC assessment methodology developed with FST enhance information security in the organization?

In seeking answers to RQ1 and RQ2, the following research hypotheses (H) were derived:

H1: An ISC assessment methodology that is constructed using FST contemplates all-inclusive ISC scenarios; employs a less-subjective, precision/accuracy-based method; prevents or eliminates the random and unnecessary selection of ISC; and considers organizations' restrictions and constraints when assessing ISC.

H2: An ISC assessment methodology developed with FST that addresses the weaknesses identified in traditional assessment methodologies enhances information security in the organization.

Based on the information, arguments, and claims presented above, the research model is illustrated in Figure 2.

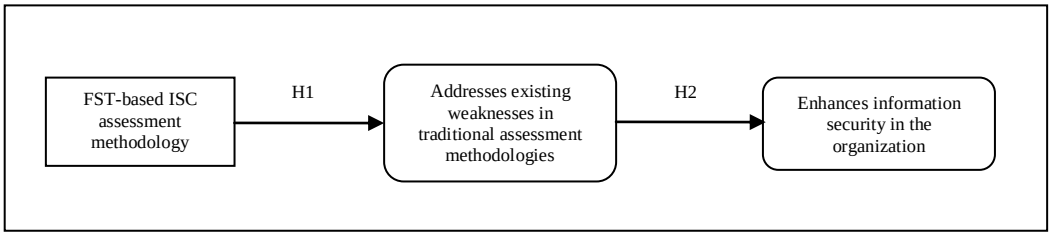



**Figure 2.** Relationship Between a FST-based ISC Assessment Methodology and Information Security in the Organization

## 1.4 Relevance and Significance

It is essential that organizations adjust their information security to meet a reasonably expected security level. Organizations should assess regularly their information security in order to ensure the safety of their information assets. Nonetheless, since there is a large number of ISC that can be selected and implemented, organizations usually do not know

which ISC are the most effective in protecting their information. The evaluation and prioritization of ISC conducted within this dissertation, therefore, constitute a strategic decision making problem. An assessment methodology that evaluates and prioritizes ISC effectively, in a more precise manner, is undoubtedly of interest to many organizations.

When evaluating ISC, organizations must evaluate and prioritize them in order to satisfy their IT security requirements (Da Veiga & Eloff, 2007; Karyda, Kiountouzis, & Kokolakis, 2004; Barnard & von Solms, 2000). Equally important, organizations do not have the luxury of implementing all available ISC due to a variety of organizational-specific constraints (e.g., costs, resources availability, scheduling restrictions, etc.). ISC assessment methodologies, such as the one built in this dissertation, must need to be available to assist organizations when evaluating and prioritizing ISC.

The evaluation process referred to above must be performed carefully in order to fit the specific needs of the organization, as there is no single IT solution that can fit all organizations (Whitman, Towsend, & Aalberts, 2001). Additionally, the assessment methodology developed herein precisely evaluates and prioritizes ISC, according to organizations' specific requirements and criteria, as well as generates more accurate assessment scores, representing a valid and significant contribution to the information security literature.

Moreover, except for studies performed by Zlateva, Velev, and Zabunov (2011) and Schryen (2010), which used fuzzy logic to estimate real estate investment risks, and to present a novel fuzzy-set based decision support model for security investment decision makers, respectively, to the best of the author's knowledge, there have been no other research studies within the literature that have specifically evaluated and prioritized ISC

in organizations using FST (Otero, Ejnioui, Otero, & Tejay, 2012a; Otero, Tejay, Otero, & Ruiz, 2012b; Ejnioui, Otero, Tejay, Otero, & Qureshi, 2012). Schryen (2010) presented a unique fuzzy-set based decision support model for security investment decision makers. The author proposed a formal security language by applying propositional logic, decision theory, and FST in order to develop the decision model. Schryen (2010) further drew on computational complexity theory to analyze the complexity of the model. Zlateva et al. (2011), on the other hand, proposed a fuzzy logic model for complex estimation of real estate investment risks, based on available information sources and expert knowledge. The fuzzy logic model was designed as a hierarchical system that included several variables. Zlateva et al.'s (2011) model was intended to be implemented as a Web service in a cloud computing environment for increasing the span and efficiency of real estate manager activities.

Based on the above, an assessment methodology that precisely evaluates and prioritizes ISC using FST represents a valid contribution to the information security literature and is of significant interest to organizations. The methodology developed in this dissertation adds practical value, as it helps organizations in dealing with the information security problem by accurately identifying which ISC need to be selected, and eventually implemented in order to ensure adequate protection of the information.

### 1.5 Definitions of Terms

The following definitions are provided to ensure a clear understanding of some specific terms used throughout this dissertation.

*Best Practices*: Control Objectives for Information and related Technology (COBIT) 4.1 defines best practices as proven activities or processes that have been successfully used by multiple organizations.

*Design-Science Research*: refers to, based on Hevner, March, Park, and Ram (2004), a problem-solving paradigm. Hevner et al. (2004) also refer to Denning (1997) and Tsichritzis (1998) when stating that Design-Science Research "seeks to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management, and use of information systems can be effectively and efficiently accomplished" (p. 76).

*Fuzzy Set Theory*: Based on Zimmermann (2001), Fuzzy Set Theory "provides a strict mathematical framework …in which vague conceptual phenomena can be precisely and rigorously studied" (p. 318). Fuzzy Set Theory is utilized to model situations in which fuzzy relations, criteria, and phenomena exist (Zimmermann, 2001).

*Fuzzy Logic*: allows logical reasoning with partially true imprecise statements (Das, 2009). In other words, in fuzzy logic, propositions can be true to some degree; meaning that truth values are no longer restricted to the two values 'true' and 'false', but expressed by the linguistic variables 'true' and 'false' (Zimmermann, 2010). Fuzzy logic is a complex mathematical method that allows solving difficult simulated problems with many inputs and output variables.

*Information*: defined as an asset essential to organizations which needs to be suitably protected. It can exist in many forms (e.g., printed or written on paper, electronically stored, transmitted using electronic means, shown on films, spoken in conversations, etc.)

(British Standard International Organization for Standardization (ISO) / International Electro technical Commission (IEC) 27002, 2005).

*Information Security*: according to the ISO/IEC 27002 (2005), refers to "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (p. viii). Security of information is achieved by implementing a suitable set of procedures or controls, including, but not limited to, policies, processes, guidance, best practices, and organizational structures, among others.

*Information Security Controls*: include policies, processes, guidance, best practices, organizational structures, and software and hardware functions, among others. These controls are established, implemented, monitored, reviewed, and enhanced, where necessary, to ensure that (1) specific information security business objectives are achieved, as well as (2) information security risks are addressed or mitigated (ISO/IEC 27002, 2005).

*Organization*: defined per COBIT 4.1 as the manner in which an enterprise is structured (i.e., entity).

*Risk*: in business terms, COBIT 4.1 defines it as the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets. It is usually measured by a combination of impact and probability of occurrence.

**1.6 Summary**

Chapter one stressed how critical information security is to organizations given the current high use and dependence of computers and information systems. Specific facts and figures identified by the FBI, the CSI/FBI Computer Crime and Security Survey, and

the literature related to fraud schemes and information security breaches, among others, were mentioned and discussed. Such alarming facts and figures give rise to inadequacies and inefficiencies in regards to information security practices, while also serve as motivation for finding innovated ways to assist organizations improve their capabilities for securing their valuable information.

As seen above, the literature argues that the current use of information security tools and technologies (encryption, firewalls, access management, etc.) alone is not sufficient to protect the information and address information security challenges. Another major step towards the protection of information is the implementation of ISC. Nevertheless, due to a variety of constraints (e.g., costs, availability of resources, etc.), business objectives, organizational-specific criteria, etc., organizations can not implement all possible ISC. More importantly, when reviewing traditional approaches and methodologies used for ISC assessments in organizations, the literature shows several issues, gaps, weaknesses, and/or inadequacies among these assessment methodologies that prevent an effective ISC evaluation in organizations. This research aimed to develop an ISC assessment methodology that adequately address the existing weaknesses identified in traditional ISC assessment methodologies, resulting in a more effective selection of ISC and, in turn, enhanced information security in organizations. The aforementioned represents the problem that was investigated throughout this research effort. An effective evaluation of ISC must ensure that only the best and most appropriate ISC get implemented. Adequate selection and implementation of ISC reduce opportunities for information system failures, potentially improving the overall

information security in organizations. Development of such assessment methodology constitutes a significant contribution to the information security literature.

Consistent with the above, the goal of this dissertation was to develop an assessment methodology that considers all-inclusive ISC evaluation scenarios, adequately accounts for organizations' restrictions and constraints; significantly minimizes subjectivity and ambiguity; and prevents unnecessary and random ISC selections. To this end, various research questions and hypotheses were created and proposed, respectively.

The research problem stated above was of great relevance and significance to organizations as they constantly find themselves looking for ways to adjust their information security plan and strategy in order to meet a reasonable information security level. As a result, the assessment methodology developed herein that evaluates and prioritizes ISC effectively, in a more precise manner, is undoubtedly of interest to many organizations. The methodology helps organizations in dealing with the aforementioned information security problem by accurately identifying which ISC need to be selected, and eventually implemented in order to ensure adequate protection of the information.

From here on, this dissertation is organized as follows. Chapter two reviews and discusses the literature related to the evaluation of ISC in organizations. Chapter three describes the research methodology as well as the specific research method employed. Chapter three also explains the theory adopted for developing the ISC assessment methodology instrument, and presents the data collection method and the rationale for its adoption. Chapter four presents and discusses the results of this dissertation, while Chapter five concludes this dissertation by providing the conclusions, implications, recommendations, and summary, among others, as a result of the investigation process.

# Chapter 2

# Review of the Literature

## 2. Introduction

The purpose of this Chapter is to discuss and review the literature related to the evaluation of ISC in organizations. Following is a detailed description of the approaches and methodologies that have been used in organizations in regards to ISC evaluations, including several weaknesses and inadequacies identified within them.

## 2.1 Risk Analysis and Management

Based on Barnard and von Solms (2000), the process of identifying, selecting, and prioritizing ISC 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 (Methodology 1) consists of performing business analyses as well as risk assessments, resulting in the identification of information security risks (i.e., requirements) (Barnard & von Solms, 2000). RAM would then list the information security requirements as well as the proposed ISC 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 necessarily taking into account organizations' specific constraints. For example, through performing RAM, an organization may identify 30 ISC. Nonetheless, the organization may not be able to implement effectively the 30 ISC due to costs and scheduling constraints, among others. Moreover, there may not be enough resources within the organization to ensure the 30 ISC are effectively put in

place. In this particular case, organizations list all ISC identified and subjectively determine how critical each individual ISC is, while considering costs versus benefit analyses. The weakness just described prompts organizations to explore new ways to determine and measure the relevancy of ISC.

According to Dhillon and Torkzadeh (2006), there is no doubt that RAM has proved useful in ensuring information security. In fact, in cases where security-related incidents have occurred in the past, and calculation of costs is reasonable, RAM has proven to be very practical. Nonetheless, RAM is not identified as the best or fundamental mean to ensure information security. Dhillon and Torkzadeh (2006) state that organizations, when performing RAM, establish controls that are either unnecessary or relate to trivial issues. Furthermore, exclusive reliance on RAM has often been criticized since it has proven to be more problematic for maximizing information security rather than beneficial.

**2.2 Baseline Manuals / Best Practice Frameworks, Ad-Hoc Approach**

Baseline manuals or best practice frameworks (Methodology 2) are approaches widely used by organizations to introduce ISC in organizations (Barnard & von Solms, 2000). Saint-Germain (2005) states that best practice frameworks assist organizations in identifying and selecting ISC. Some best practices include: COBIT, Information Technology Infrastructure Library (ITIL), Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), and the National Institute of Standards and Technology (NIST). Da Veiga and Eloff (2007) also mention other best practice frameworks which have assisted the identification and selection of ISC. These practice frameworks are: ISO/IEC 177995 and ISO/IEC 27001, and ISO/IEC 27002, PROTECT, Capability Maturity Model (CMM), and Information Security Architecture (ISA).

In Siougle and Zorkadis (2002), a baseline manual selection process was created to provide data controllers with a framework for selecting appropriate ISC that satisfy privacy protection legislation requirements, as well as the security and privacy objectives of an organization. National and European data protection laws regulate the processing of personal data and impose serious obligations to data controllers for their protection and secure processing. Therefore, the response of organizations to data protection law provisions and related user interests become determining factors, as well as improve acceptance of their business services. Given the above, Siougle and Zorkadis (2002) developed a model that would select ISC from a baseline manual, satisfying the legal privacy protection requirements and any particular privacy requirements of the data controller regarding the secure processing of personal data.

The process of selecting the most effective ISC from baseline manuals or best practice frameworks is a challenging one (van der Haar & von Solms, 2003). Van der Haar and von Solms (2003) state that baseline manuals or best practice frameworks leave the identification of ISC to the user, while offering little guidance in terms of determining the best controls to provide adequate information security for the particular business situation. Additionally, identification of ISC via baseline manuals or best practice frameworks does not necessarily take into consideration organization specific constraints, such as, costs, scheduling, and resource constraints, among others. Other less formal methods used, such as, ad hoc or random approaches (Methodology 3), could also lead to the inclusion of unnecessary ISC or exclusion of required ISC (Barnard & von Solms, 2000).

### 2.3 Information Security Checklists

Another method to identify and select ISC in organizations is through completing checklists (Methodology 4). Chen and Yoon (2010) used checklists as a framework to identify common ISC, including information security risks, within cloud-based organizations. The checklists were to be used by both, internal and external auditors, in assuring a secure computing environment. Chen and Yoon (2010) completed checklists for the Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) delivery service models within a public cloud. Checklists were also completed for the community and private deployment models. The hybrid deployment model and the Platform-as-a-Service delivery service model were not included within the checklists as Chen and Yoon (2010) opted to address those in the future. Table 1 shows the issues specifically addressed by Chen and Yoon's (2010) developed information security checklists.

Numerous information security checklists have been proposed and used over the years (Baskerville, 1993). Their importance, according to Dhillon and Torkzadeh (2006), has been focused on identifying "all possible threats to a computer system and propose solutions that would help in overcoming the threat" (p. 294). Nonetheless, Dhillon and Torkzadeh (2006) stressed that over the years the significance of information security checklists has declined simply "because they provide little by way of analytical stability" (p. 294). Based on interviews conducted by Dhillon and Torkzadeh (2006) on information security managers, checklists are not considered to be the essence of information security. Even though checklists may be viewed as good means to ensure information security, exclusive reliance on them could result in a flawed information systems security strategy (Dhillon & Torkzadeh, 2006). Furthermore, Backhouse and

Table 1. Checklists completed by Chen and Yoon (2010) to identify ISC

| Model | Issues addressed by Information Security Checklist |
|---|---|
| IaaS | Data location aware, data ownership aware, data protection plan and best practice, data processing isolation, data lock-in, IaaS IT architecture, regulatory compliance, cloud IT technique, reporting control, cloud disaster recovery plan, cloud business continuity, and overall IT projects costs. |
| SaaS | Data activity surrender, format, monitoring for availability, and performance. |
| Community | Community cloud IT architecture, cloud management, and exit strategy. |
| Private | Private cloud IT architecture, private cloud reporting control, and disaster recovery / continuity plan. |

Dhillon (1996) argued that although checklists draw concern on particular details of procedures, they do not completely address the key task of understanding the substantive questions. Checklists are concerned on what can be done without any analytical stability in regards to the kind of actions identified (Baskerville, 1993).

### 2.4 Control Selection Process

Barnard and von Solms's (2000) formalized control selection process (CSP) (Methodology 5) approach for the selection and evaluation of ISC included a process that eliminated the need for a random selection; as well as integrated information security policies to formally identify ISC from the ISO/British Standard (ISO/BS) 7799 best practice framework. In particular, Barnard and von Solms's (2000) business analysis included a set of high-level business oriented questions that analyzed the specific business situation, and determined how important information security and information security management were to the particular organization. The above resulted in the determination of information security requirements that proposed the particular information security policy to be introduced in the organization. Each of the security requirements dictated one or more information security policy statements that became part of the overall organization's information security policy. Each policy statement

within the information security policy was enforced by one or more ISC from the ISO/BS 7799 best practice framework.

Barnard and von Solms (2000) argued that their proposed CSP approach of formalizing business analyses into security requirements and, eventually, information security policies is essential for identifying ISC. Nevertheless, this ISC selection process although eliminated the need for a random selection, still involved a high degree of subjectivity when determining which ISC will be ultimately selected. An ideal case would be if all processes involved (i.e., from business analyses to the selection of ISC) could be tightly integrated into one formalized process subject to a methodological approach that would address the subjectivity factor, thus, providing for a more accurate ISC evaluation (Barnard & von Solms, 2000).

**2.5 Desirability Functions**

In Otero, Otero, and Qureshi (2010), an innovative ISC evaluation and selection approach was developed to help decision makers select the most effective ISC in resource-constrained organization environments. The proposed approach used desirability functions (Methodology 6) to quantify the desirability of each ISC after taking into account benefits and restrictions associated with implementing the particular control. The above provides organizations with a measurement that is representative of the overall quality of ISC based on organizational goals. Through a case study, the approach proved successful in providing a way for measuring the quality of ISC (based on multiple application-specific criteria) in organizations.

Otero et al.'s (2010) methodology took into consideration relevant quality attributes of ISC in order to determine their relative importance. This allowed an ISC prioritization

scheme that represented how well ISC met quality attributes, and how important those quality attributes were for the specific organization. Desirability was defined in terms of different features, where each feature was determined by the organization to either be present or not. Once all features were identified, each individual ISC was evaluated against each feature using a simple binary (boolean) scale (i.e., 0 or 1). ISC that satisfied the highest number of features exposed a higher level of quality (or priority) for that particular quality attribute.

Even though the above resulted in an ISC evaluation/prioritization approach based on how well ISC met quality attributes, and how important those quality attributes were for the organization, a boolean criteria for evaluating the quality attributes of ISC in order to determine which ones to select, may not be considered a precise enough assessment for selecting, and ultimately implementing ISC in organizations.

### 2.6 Information Security Control Attribute Profile

In van der Haar and von Solms (2003), a model was developed to derive the optimal set of control attributes, called the Information Security Control Attribute Profile (ISCAP) (Methodology 7) that in the end would assist the selection of ISC. The authors examined attribute profiles to support the selection of ISC in organizations. Specifically, they required organizations to obtain a set of attributes that should accompany every ISC before being selected. Examples of these attributes included: strength; correct installation; rules and procedures; clearance; and acceptance criteria. According to van der Haar and von Solms (2003), before determining whether an ISC should be selected, each ISC should have characteristics or attributes in place such as the above.

As stated by van der Haar and von Solms (2003), identification of optimal security characteristics for every ISC is crucial prior of being selected to ensure their effective and continuous operation. In order to address the relevance of ISC, van der Haar and von Solms's (2003) ISCAP approach was based on the diversity and unique properties of organizations, the environment that renders a security control adequate, the organization's information security goals and objectives, and the attributes that can support information security. Through their ISCAP model, determination of the attributes which ultimately would result in the selection of ISC was based on feedback gathered from organization personnel, stating whether the information security attribute was either present or not. Formalizing the ISCAP model into one methodological approach that addresses the subjectivity involved when evaluating ISC in organizations, would provide for a more accurate assessment of ISC.

### 2.7 Information Security Risk-Control Assessment Model

Ou Yang, Shieh, and Tzeng (2011) proposed an information security risk-control assessment model (ISRCAM) (Methodology 8) to improve information security for companies and organizations. Specifically, the authors developed an information security risk-control assessment model that combined the Multi-criteria Optimization and Compromise Solution technique (also known as VIKOR in Serbian), the analytic network process (ANP), and the decision-making trial and evaluation laboratory (DEMATEL), all together, to assess the performance and validate the effectiveness of already-implemented ISC in organizations and, thus, improve overall information security.

VIKOR is based on an aggregating function that represents closeness to the ideal, and was employed to rank risk-control areas and risk values (Ou Yang et al., 2011). Ou Yang

et al. (2011) state that the "VIKOR method introduced the multicriteria ranking index based on a particular measure of 'closeness to the ideal/aspired level' and was introduced as an applicable technique within Multiple Criteria Decision Making" (p. 2). VIKOR then ranks a set of choices in the presence of conflicting criteria, assisting decision makers in selecting the best alternative (Opricovic & Tzeng, 2007).

The ANP is derived from the Analytic Hierarchy Process (AHP) (Saaty, 1980), and has been used in Multiple Criteria Decision Making (MCDM) problems to relax restrictions on hierarchical structure. Saaty (1996) proposed ANP as a new MCDM method in order to resolve the problems of interdependence and feedback among criteria and alternatives in real-world cases. ANP accounts for clusters with similar weights (contrary to traditional normalization methods), dealing with different degrees of influence among the clusters of criteria in real world situations. Ou Yang, Shieh, Leu, and Tzeng (2008) indicate that "the assumption of equal weights for each cluster to obtain the weighted supermatrix is unrealistic and needs to be improved" (p. 2). As a result, Ou Yang et al. (2011) used DEMATEL results to improve the normalization process within ANP. DEMATEL was used not only to construct the interrelations between criteria in building the Ou Yang et al.'s (2011) network relations map, but also to improve the normalization process of ANP (Fontela & Gabus, 1976; Gabus & Fontela, 1972). A hybrid model such as the ISRCAM above has been successfully used in several fields (Tzeng, Chiang, & Li, 2007; Liou, Tzeng, & Chang, 2007).

Biery (2006), however, stated that the risk management process is an ongoing process composed of phases, such as, risk assessment; risk remediation; risk monitoring and review; and risk management enhancement. Ou Yang et al.'s (2011) research above

regarding the ISRCAM focused on improving the risk monitoring and review phase by proposing a risk-control assessment method to improve controls and reduce risk. The purpose of their research was to develop an assessment model for evaluating and monitoring previously implemented ISC to ensure the safety of information assets. An empirical example for information security risk control assessment was presented to illustrate the proposed method. Nonetheless, Ou Yang et al.'s (2011) research study did not address the selection of ISC, as their work assumed that ISC had already been put in place by the organization. Instead, their work was focused on assessing the performance and validating the effectiveness of already-implemented ISC, rather than evaluating from an initial, all-inclusive set of ISC, and determining which ones are the best to implement.

**2.8 Information Security Risk Management Method**

In Lv, Zhou, and Wang (2011), an information security risk management method (ISRMM) (Methodology 9) was developed for ranking ISC quantitatively with the help of the PROMETHEE methodology, and the GAIA plane. The PROMETHEE method is a multi-criteria analysis method based on pair wise comparisons (Lv et al., 2011). The authors introduced the PROMETHEE methodology into the field of information security, and proposed a ranking method for different types of ISC measurements by establishing a group decision model. A multi-attribute model was designed based on the PROMETHEE method to evaluate ISC to certain risks from several aspects provided by decision maker preferences. A ranking of the measures was given accordingly, and a sensitivity analysis was put forward based on the GAIA module, which considers specific organizations' criteria and shows a graphical visualization tool for analyzing the ISC. The criteria used included the cost of operating the security measurements, the effectiveness of the solution

to reduce risks, social ethics, the organization security demand, and other requirements the decision maker was concerned with.

Lv et al.'s (2011) contribution included a control ranking model which considered multiple criteria analyses as well as the interests of decision makers for an information security control plan to be implemented. However, as noted by the authors, even though the expectation of every decision maker is to identify ISC that optimize all criteria, there is still no absolute best solution, and the selection of ISC based on Lv et al.'s ISRMM methodology mainly depended on the decision maker's preference, resulting in the potential selection of unnecessary ISC, or the exclusion of required ones. As seen, subjectivity was a major contributing factor in Lv et al.'s (2011) selection of ISC research study. In other words, decision makers employed a high degree of subjectivity when implementing ISRMM to determine the criticality of each individual ISC before its selection. Organizations must continue to explore new assessment methods to precisely and accurately measure the relevancy of each ISC before determining their selection.

**2.9 Legal Requirements Determination Model**

In another study, Gerber and von Solms (2008) created a Legal Requirements Determination Model (LRDM) (Methodology 10) for defining legal requirements, which in turn, indicated relevant ISC to be selected from the list provided in the ISO/IEC 27002 best practice framework to satisfy the identified legal requirements. Specifically, the authors: (1) developed a structured model to assist in establishing information security requirements from a legal perspective; (2) provided an interpretation of the legal source associated with information security requirements; and (3) proposed potential ISC 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 ISC from the ISO/IEC 27002 framework was produced to satisfy the previously identified legal requirements.

Nonetheless, as identified and evidenced earlier, the selection of ISC 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.

## 2.10 Grey Relational Analysis

In Otero et al. (2012a), a methodology that used Grey Relational Analysis (GRA) (Methodology 11) was developed to solve a multi-attribute decision making problem that consisted of evaluating relevant quality attributes and features of ISC, and selecting the best (high ranked) set based on those attributes and features.

Otero et al.'s (2012a) GRA assessment methodology used grey systems theory as the basis for its development. The theory has been effective for decision problems with imprecise or ambiguous data leading to conflicting situations in which the evaluation of

alternatives becomes difficult. Such is the case when selecting and implementing ISC in organizations. Grey systems theory, according to Liu and Lin (2011), has also provided significant contributions in related areas such as:

- Grey algebraic systems, grey equations, and grey matrices;
- Sequence operators and generation of grey sequences;
- System analysis based on grey incidence spaces and grey clustering;
- Grey prediction models;
- Decision making using grey target decision models; and
- Optimization models using grey programming, grey game theory, and grey control.

Otero et al. (2012a) performed a case study to implement and evaluate the methodology. The first step involved identifying a set of ISC that could be implemented in the organization. These ISC were obtained from the ISO/IEC 27002 standard best practice framework, which includes an all-inclusive list of ISC that can potentially be selected and implemented. The second step identified relevant quality attributes related to information security and used them as evaluation criteria for all potential ISC. The attributes were defined in terms of different features, where the importance of each feature was expressed as a grey number. In practical applications, a grey number represents an indeterminate number that takes its possible value from an interval or a set of numbers.

ISC that satisfied the highest number of features exposed a higher level of quality for that particular attribute. Once all ISC were evaluated and measurements computed for all quality attributes and features, the methodology used the Euclidean distance between ISC

being evaluated and ideal ISC to fuse all measurements into one unified value that was representative of the overall quality of the ISC. The resulting ranking of each ISC was derived based on the goals and specific needs of the organization.

As seen, Otero et al.'s (2012a) evaluation of ISC was fully dependent on the particular organization and its information security objectives. Through a case study, the methodology was proven successful in providing a way for measuring the quality of information security controls based on multiple application-specific criteria. In regards of contributions, first, the methodology is relatively simple, can be easily implemented in a spreadsheet or software tool, and promote usage in practical scenarios where highly complex methodologies for ISC selection may become impractical. Second, the methodology fuses multiple evaluation criteria and features to provide a holistic view of the overall ISC quality. Third, and probably the most meaningful contribution from a practical standpoint, the methodology is easily extended to include additional attributes and features, and can evaluate ISC in various domains. Overall, the methodology proved to be a feasible technique for evaluating ISC in organizations.

Otero et al. (2012a) noted, however, that their methodology did not consider the true degree of relevance (imprecise in nature) when evaluating ISC. Subjectivity was still a factor when evaluating attributes and features of ISC to base their ultimate selection. The above still represents a major problem for organizations that can potentially impact the overall security over the information. While grey numbers can handle easily ambiguous and imprecise data, grey systems still do not provide the powerful analytical tools available in, for instance, FST, which allows for a more accurate, less-subjective assessment of imprecise parameters. Otero et al. (2012a) acknowledged that the

development of an assessment technique, based on FST, can better tackle challenging problems with imprecise data such as ISC evaluations. An ISC assessment methodology based on FST provides benefits and advantages over traditional methods, including a strict mathematical methodology that can precisely and rigorously examine vague conceptual phenomena (Zimmermann, 2010). FST has been used as a modeling, problem solving, and data mining tool, and has proven superior to existing methods as well as attractive to enhance classical approaches.

Based on the thorough literature review presented above, which resulted from numerous search queries (including backward and forward search reviews) that included keywords, such as, information security controls; selection, evaluation, or assessment; organizations; and information security; among others, and to the best of the author's knowledge, there have been no other studies within the literature that have addressed the evaluation and selection of ISC in organizations. Table 2 summarizes the literature review just presented, pointing out the weaknesses/inadequacies of the aforementioned ISC assessment methodologies.

As stated, the literature clearly evidences weaknesses in existing assessment methodologies for ISC in organizations. Risks resulting from those weaknesses may include inaccurate or incomplete processing of data; unauthorized access to data that might destroy or manipulate data (or report logic) in a fraudulently or unintentionally way; as well as the potential loss of data or inability to access data as required (Public Company Accounting Oversight Board (PCAOB)). To support the above, in September of 2011, investment banking company, UBS, lost more than $2 billions on unauthorized trades, resulting from unauthorized access or access gained beyond necessary ones, by a

Table 2. Weaknesses of literature-based ISC assessment methodologies

| | ISC Assessment Methodology | Description of Weakness/Inadequacy |
|---|---|---|
| 1. | Risk Analysis and Management (RAM) (Barnard & von Solms, 2000; Dhillon & Torkzadeh, 2006) | - RAM has been described as a subjective, bottom-up approach (van der Haar & von Solms, 2003), not taking into account specific organizations' constraints (Barnard & von Solms, 2000).<br>- Per Dhillon and Torkzadeh (2006), when organizations perform RAM, controls that are either unnecessary or relate to trivial issues are implemented.<br>- Exclusive reliance on RAM has proven to be more problematic than beneficial for maximizing information security (Dhillon & Torkzadeh 2006). |
| 2. | Baseline Manuals or Best Practice Frameworks (COBIT, ITIL, OCTAVE, NIST, ISO / IEC 177995, ISO/IEC 27001, and ISO/IEC 27002, PROTECT, CMM, and ISA) (Barnard & von Solms, 2000; Saint-Germain, 2005; Da Veiga & Eloff, 2007; Siougle & Zorkadis, 2002) | - Baseline manuals or best practice frameworks leave the identification of ISC to the user, while offering little guidance in terms of determining the best ISC to provide adequate security for the particular business situation (van der Haar & von Solms, 2003).<br>- Baseline manuals or best practice frameworks do not necessarily account for organization specific constraints, such as, costs, scheduling, and resource constraints, among others (Barnard & von Solms, 2000). |
| 3. | Ad Hoc or Random Approach (Barnard & von Solms, 2000) | - Ad hoc or random approaches lead to the inclusion of unnecessary ISC and/or exclusion of required ISC (Barnard & von Solms, 2000). |
| 4. | Information Security Checklists (Chen & Yoon, 2010; Dhillon & Torkzadeh, 2006; Baskerville, 1993; Backhouse & Dhillon, 1996) | - Dhillon and Torkzadeh (2006) stress that the significance of information security checklists has declined simply "because they provide little by way of analytical stability" (p. 294).<br>- Exclusive reliance on checklists could result in a flawed information systems security strategy (Dhillon & Torkzadeh, 2006).<br>- Backhouse and Dhillon (1996) indicate that checklists do not completely address the key task of understanding the substantive questions.<br>- Checklists are concerned on what can be done without any analytical stability in regards to the kind of actions identified (Baskerville, 1993). |
| 5. | Control Selection Process (Barnard & von Solms, 2000) | - Barnard and von Solms' (2000) control selection process although eliminated the need for a random selection, still involved a high degree of subjectivity in the determination of which ISC will be ultimately selected.<br>- Lack of integration of all processes involved (i.e., from business analyses through ISC selection) into one formalized methodological approach that would adequately address subjectivity (Barnard & von Solms, 2000). |

Table 2. (Continued). Weaknesses of literature-based ISC assessment methodologies

| | ISC Assessment Methodology | Description of Weakness/Inadequacy |
|---|---|---|
| 6. | Desirability Functions (Otero et al., 2010) | - A boolean criteria for evaluating the quality attributes of ISC in order to ultimately determine which ones to select may not be considered a precise enough (less-subjective) assessment for selecting ISC in organizations (Otero et al., 2010). |
| 7. | ISC Attribute Profile (van der Haar & von Solms, 2003) | - The objective of van der Haar and von Solms' (2003) developed model was to identify security characteristics that would be crucial for every ISC prior of being selected to ensure their effective and continuous operation.<br>- Determination of security attributes that resulted in the selection of ISC was based strictly on feedback gathered from organization personnel, stating whether the information security attribute was either present or not. Formalizing the above into one methodological approach that addresses the subjectivity involved when evaluating ISC would provide for a more accurate assessment of ISC. |
| 8. | Information Security Risk-Control Assessment Model (Ou Yang et al., 2011) | - Ou Yang et al.'s (2011) work was focused on assessing the performance and validating the effectiveness of ISC already implemented instead of evaluating from an initial, all-inclusive pool of ISC, and determining which ones to implement.<br>- Ou Yang et al.'s (2011) research study did not address the initial selection of ISC, as they assumed that ISC had already been put in place in the organization. |
| 9. | Information Security Risk Management Method (Lv et al., 2011) | - Selection of ISC mainly depended on the decision maker's preference (Lv et al., 2011).<br>- Subjectivity was a major factor employed by the organization to determine the criticality of each individual ISC before its selection. |
| 10. | Legal Requirements Determination Model (Gerber & von Solms, 2008) | - Baseline manuals or best practice frameworks leave the identification of ISC to the user, while offering little guidance in terms of determining the best ISC to provide adequate security for the particular business situation (van der Haar & von Solms, 2003).<br>- Baseline manuals or best practice frameworks do not necessarily account for organization specific constraints, such as, costs, scheduling, and resource constraints, among others (Barnard & von Solms, 2000). |
| 11. | Grey Relational Analysis (GRA) (Otero et al., 2012a) | - The GRA methodology did not consider the true degree of relevance (imprecise in nature) when evaluating ISC, as subjectivity was still a factor involved in the evaluation (Otero et al., 2012a).<br>- GRA lacks the powerful analytical tools available in FST, which allows for a more accurate, less-subjective assessment of imprecise parameters. |

rogue trader (Kantšukov & Medvedskaja, 2013). Various months after that, in early 2012, card processor Global Payments, Inc., a provider of electronic transaction processing

services for merchants, financial institutions, government agencies and multi-national corporations, among others, experienced its second data breach in less than 12 months involving sensitive customer information for millions of cardholders (Cheney, Hunt, Jacob, Porter, & Summers, 2012).

Figure 3 illustrates the weaknesses listed earlier, as well as some of the risks just mentioned that those weaknesses may translate into. Most importantly, Figure 3 shows the significant contribution of the proposed ISC assessment methodology by addressing the weaknesses identified and preventing and/or avoiding the potential risks illustrated, resulting in a more effective selection of ISC and, in turn, enhanced information security in organizations (research problem).

Table 3 further summarizes and combines the weaknesses into five and present them in question format. Table 3 also shows the relationship between the traditionally-used ISC assessment methodologies reviewed above (referred to as 'M' in the table) and each weakness listed. That is, a "-" sign in Table 3 indicates that the methodology does not address the weakness in question (i.e., the weakness is present in the assessment Methodology); whereas a "+" sign indicates that the methodology does address the weakness. A more significant purpose of Table 3 is that it supports how a FST-based methodology (last column on the right) addresses all of the weaknesses identified from the literature and, by doing this, how will it contribute favorably to the information security literature.

As evidenced above, the FST-based ISC assessment methodology is expected to (a) enhance current evaluation processes for the initial selection of ISC in organizations; (b) employ a less-subjective, precision/accuracy-based method; (c) eliminate or prevent the

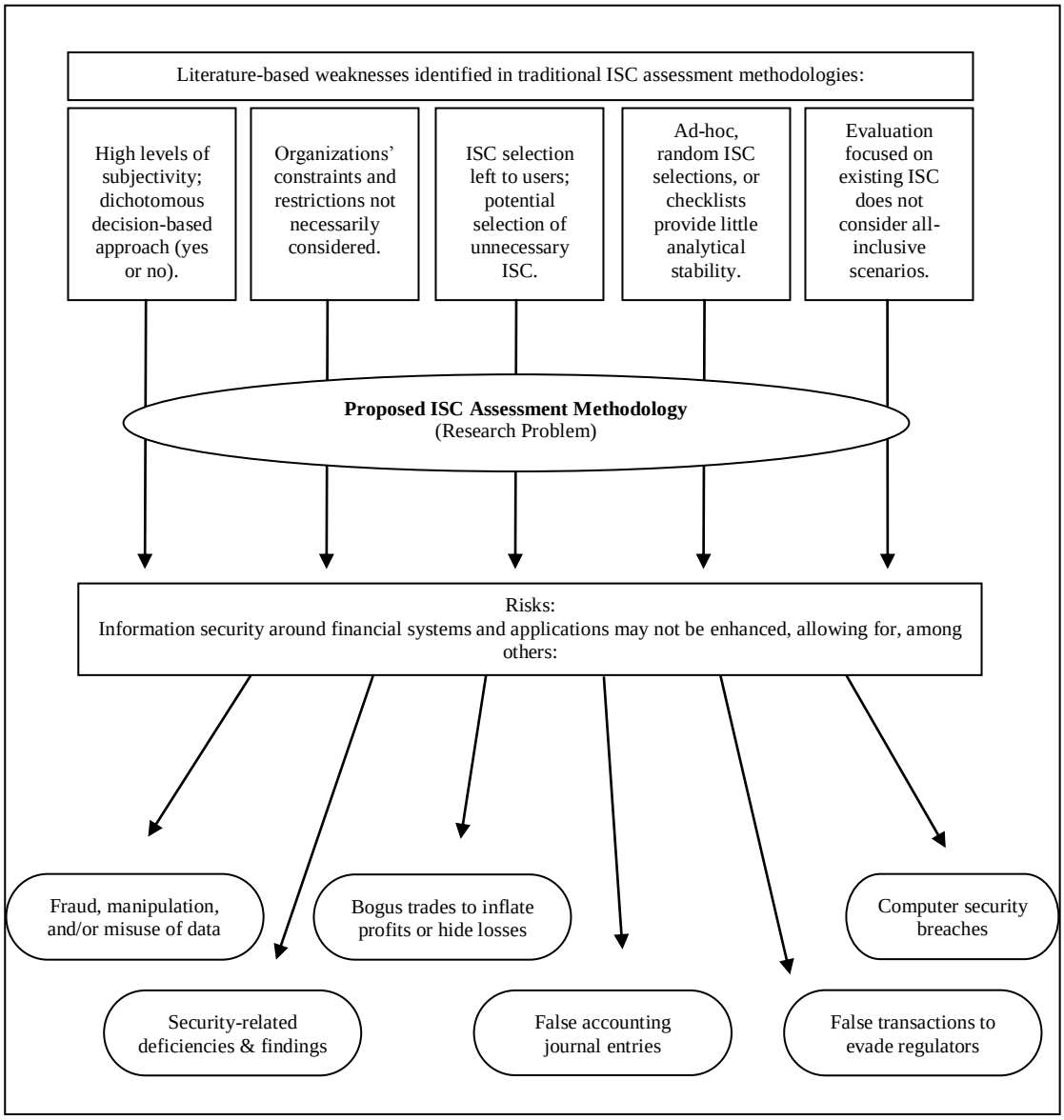



**Figure 3.** Weaknesses, risks, and significance of the research problem

random and unnecessary selection of ISC; (d) consider organizations' restrictions and constraints; and (e) improve the overall information security in organizations. Equally significant, a FST-based assessment methodology allows for the modeling of imprecise parameters (i.e., criteria for determining ISC relevance), resulting in a more accurate assessment, which is crucial to determine the best ISC. Surprisingly, such a methodology

Table 3. Relationship between ISC assessment methodologies and literature-supported weaknesses (a "-" sign indicates that the ISC assessment methodology does not address the weakness in question, while a "+" sign does)

| **Weakness/Inadequacy** | **M1** | **M2** | **M3** | **M4** | **M5** | **M6** | **M7** | **M8** | **M9** | **M10** | **M11** | **FST** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Minimizes subjectivity significantly? (van der Haar & von Solms, 2003) | - | - | - | - | - | - | - | + | - | - | - | + |
| Considers organizations' restrictions and constraints? (van der Haar & von Solms, 2003) | - | - | - | + | - | + | + | + | + | - | + | + |
| Prevents selection of unnecessary ISC? (Dhillon & Torkzadeh, 2006; Barnard & von Solms, 2000) | - | - | - | - | + | + | + | + | - | - | + | + |
| Eliminates random selection? (Barnard & von Solms, 2000; Dhillon & Torkzadeh, 2006; Saint-Germain, 2005; Da Veiga & Eloff, 2007; Siougle & Zorkadis, 2002; Baskerville, 1993; Otero et al., 2010; van der Haar & von Solms, 2003; Ou Yang et al., 2011; Lv et al., 2011; Gerber & von Solms, 2008) | + | + | - | + | + | + | + | + | + | + | + | + |
| Consider all-inclusive, best practice ISC for evaluation rather than assessing just the ISC already in place? (Ou Yang et al., 2011) | + | + | + | + | + | - | - | - | - | + | + | + |
| Results | 2+ | 2+ | 1+ | 3+ | 3+ | 3+ | 3+ | 4+ | 2+ | 2+ | 4+ | **5+** |

has not been proposed within the information security literature. The next Chapter will describe the research methodology, including the specific research method to be employed, as well as discuss and explain the theory used for developing the ISC assessment instrument.

# Chapter 3

# Methodology

## 3. Introduction

This Chapter describes the research methodology as well as the specific research method employed. Chapter three also explains the theory adopted for developing the ISC assessment methodology, including reasons supporting its selection, as well as the underlying assumptions, and various benefits and advantages of a FST-based methodology over traditional methodologies. Moreover, Chapter three presents the data collection method and the rationale for its adoption.

## 3.1 Research Method

This dissertation follows the design-science research (DSR) method. Simon (1996) states that the DSR method is fundamentally a problem-solving paradigm. DSR creates and evaluates IT artifacts intended to solve identified organizational problems. Artifacts, as defined by Denning (1997) and Tsichritzis (1998), refer to innovations made to develop ideas, best practices, technical capabilities, and products, among others, through which the analysis, design, implementation, and use of information systems can be effectively and efficiently achieved. Nunamaker, Chen, and Purdin (1991a) further state that the process of constructing IT artifacts enables DSR researchers to understand the problem being addressed, as well as the feasibility of the artifacts' approach to the problem's solution. For purposes of this dissertation, an ISC assessment methodology (i.e., artifact) will be developed to address the existing weaknesses identified in traditional evaluation methodologies (the terms artifact and methodology will also be

used interchangeably). The new methodology is expected to deliver rich information about the research problem, as well as provide a solution (Hevner et al., 2004) by enhancing current evaluation methods, ultimately improving information security in the organization. The utilization of DSR is appropriate as it matches the purpose of this investigation which is the creation of an artifact (i.e., FST-based ISC methodology) to address a problem by providing effective and efficient solutions or improvements. Next, the various DSR guidelines or process steps are listed along with their proposed implementation.

### 3.2 DSR Guidelines / Process Steps

As mentioned, the DSR method is inherently a problem solving process. The fundamental principle of DSR is that knowledge and understanding of a design problem (and its solution) are obtained in the building and application of an artifact (Hevner et al., 2004). Hevner et al. (2004) list seven guidelines that are crucial in understanding the requirements for effective DSR. Similar to Hevner et al.'s (2004) guidelines, Vaishnavi and Kuechler (2004) also developed a general method underlying DSR. Their method included only five process steps, which represent a summarized version of Hevner et al.'s (2004) seven DSR guidelines (see Table 4). Vaishnavi and Kuechler (2004) further identified expected outputs for their five DSR process steps. Vaishnavi and Kuechler's (2004) five-process-steps General Methodology of DSR was followed in this dissertation.

### 3.3 Implementation of DSR's General Methodology

Following is a description of the five process steps from Vaishnavi and Kuechler's (2004) General Methodology of DSR, and how they will be used within the context of this dissertation.

Table 4. Hevner et al.'s (2004) DSR Guidelines and correspondent Process Steps from Vaishnavi and Kuechler's (2004) General Methodology of DSR

| **Hevner et al.'s (2004) Guidelines** | **Hevner et al.'s (2004) Guidelines Description** | **Vaishnavi and Kuechler's (2004) Process Steps** | **Vaishnavi and Kuechler's (2004) Expected Outputs** |
|---|---|---|---|
| Guideline 1 - Problem Relevance | DSR allows for the development and implementation of solutions, using appropriate technology, to address significant business problems. | Awareness of Problem | Proposal |
| Guideline 2 - Research Rigor | Rigorous methods are used by DSR to construct and evaluate the design artifact. That is, DSR requires that the artifact is rigorously defined as well as formally represented, and well-articulated. | Suggestion | Tentative Design |
| Guideline 3 - Design as Search Process | An effective artifact is searched/identified via utilizing correct actions and available resources to develop the desired solution, while addressing constraints within the problem. | | |
| Guideline 4 - Design as an Artifact | DSR results in the creation of an innovative, purposeful artifact (instantiation) in the form of a construct, model, or method. | Development | Artifact |
| Guideline 5 - Design Evaluation | Evaluation of the artifact in terms of its utility, quality, and efficacy must be rigorously performed. | Evaluation | Performance Measures |
| Guideline 6 - Research Contributions | Clear and verifiable contributions are provided in the areas of the design artifact, design foundations, and/or design methodologies. | Conclusion | Results |
| Guideline 7 - Communication of Research | Effective communication of DSR results must be presented to technical and managerial audiences. | | |

### 3.3.1 Process Step 1: Awareness of Problem

Hevner et al. (2004) define a problem as "differences between a goal state and the current state of a system" (p. 85). Awareness of problem refers to the identification of relevant needs, issues, gaps, or inadequacies that prompt for new technology-based developments to get any system from its current state to a desired, goal state. In this dissertation and as evidenced above, adequate evaluation of ISC in organizations is

determinant in relation to information security. Nevertheless, the literature points out several weaknesses in existing methodologies that prevent an effective assessment of ISC in organizations. Consistent with the aforementioned, the research problem of this investigation calls for the creation of an ISC assessment methodology that adequately addresses existing weaknesses identified in traditional ISC assessment methodologies, resulting in a more effective selection of ISC. Moreover, a new ISC assessment methodology that accounts for the weaknesses identified in traditional assessment methodologies will better assist organizations in mitigating information security risks, ultimately enhancing overall information security. The above is consistent with the expected output of this first process step: Proposal of a new research effort.

### 3.3.2 Process Step 2: Suggestion

Suggestion represents an integral part of the DSR's General Methodology, and refers to recommended (or suggested) solutions, based on existing knowledge or theory base, that can potentially address the problem at hand (Peirce, 1931). This process step involves the engaging of rigorous research methods, utilizing available means, to identify potential solutions and construct artifacts that can satisfy the problem and its constraints. Suggestion results from the proper use of knowledge base-theoretical foundations, as well as research methodologies used to discover effective solutions to problems. Hevner et al. (2004) indicate that success within this step follows exhaustive (literature) reviews and evaluations of existing tools and methodologies, including noting their advantages and disadvantages (weaknesses), before developing a new artifact. Within this dissertation, a thorough literature review has been performed in Chapter two, which is inline with, and clearly supports, the objectives of this second process step. Additionally, the FST theory adopted for designing the ISC assessment methodology, including reasons supporting its

selection, as well as its underlying assumptions, benefits, and advantages over traditional methodologies, is explained later in this chapter. The expected output for this step is the Tentative Design of a prototype solution for the stated problem.

3.3.3. Process Step 3: Development

Development consists of implementing the tentative design of a prototype solution (i.e., artifact) from process step 2. According to Hevner et al. (2004), the ultimate result of DSR is a purposeful IT artifact developed to provide a solution to a significant organizational problem. Hevner et al. (2004) define artifacts as "innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of information systems can be effectively and efficiently accomplished" (p. 83). In the context of this dissertation, the artifact built is a FST-based ISC assessment methodology, which is also the expected output of this process step. FST was used to prioritize ISC within higher-ranked information security areas identified by the organization through completing a questionnaire (data collection method; refer to *Data Collection Method and Rationale for its Adoption* section below) by fusing their respective assessment values into a single, quantified measure using the Mamdani Max-Min fuzzy reasoning technique. This provided the organization with a measurement of relevance for each ISC based strictly on specific criteria, including the organization's goals, objectives, and restrictions. The derived relevance measurement is used as the main metric for evaluating and ultimately selecting ISC.

3.3.4 Process Step 4: Evaluation

When evaluating the artifact, Hevner et al. (2004) stress that the artifact's functionality, accuracy, reliability, usability, and other relevant quality attributes must be thoroughly demonstrated via well-executed and articulated assessment methods.

Vaishnavi and Kuechler (2004) also state that evaluation of artifacts must be inline with the research problem established. The artifact must be evaluated according to performance measures (e.g., criteria, etc.) established in the research problem. This is the expected output of this process step. The evaluation phase also assists in addressing research questions and in determining whether the hypotheses drawn about the behavior of the artifact hold or not.

According to Hevner et al. (2004), there are five design evaluation methods typically used when assessing an artifact. These are: (1) Observational (case studies, field studies); (2) Analytical (static analysis, architectural analysis, optimization, dynamic analysis); (3) Experimental (controlled experiments, simulations); (4) Testing (functional, structural); and (5) Descriptive (informed arguments, scenarios).

The selection of the evaluation method must conform adequately with the artifact being created as well as the selected evaluation metrics. In this dissertation, the FST-based assessment methodology was evaluated through performing comparisons and contrasts against existing ISC assessment methodologies found in the literature (Aalst & Kumar, 2003). The evaluation method just explained refers to the "Descriptive Design Evaluation Method" (Hevner et al., 2004). This type of design evaluation method was selected over the other four evaluation methods to perform relevant comparisons and determine whether the artifact created herein enhanced existing ISC assessment methodologies, satisfying the original requirements set in the research problem.

When compared to the other four evaluation methods, the Descriptive Design Evaluation Method was critical in evaluating and comparing the artifact's suitability and effectiveness against information from the knowledge base (i.e., existing ISC assessment

methodologies found in the literature) in order to build convincing arguments and/or scenarios and demonstrate the artifact's utility.

### 3.3.5 Process Step 5: Conclusion

Conclusion is the final process step as defined by Vaishnavi and Kuechler's (2004) General Methodology of DSR. Here, results (output of this step) from the research are documented and communicated. Results are also associated with clear and verifiable research contributions from the creation of the artifact. Results either support, firmly, the objectives and direction of the investigation or simply evidence the opposite.

In regards to communication, Hevner et al. (2004) recommend presenting results to two audiences: technology and managerial audiences. When presenting to technology-oriented audiences, the artifact's benefits must be described clearly so that practitioners acknowledge them and encourage the artifact's use, as well as its further evaluation and improvement. IT practitioners must also become aware of (and understand) the process followed to create and evaluate the artifact. A full understanding of the artifact and the process used would allow effective evaluations and further extensions or improvements to the artifact. On the other hand, when communicating results to managerial audiences, Hevner et al. (2004) state that enough details must be provided for them "to determine if the organizational resources should be committed to constructing (or purchasing) and using the artifact within their specific organizational context" (p. 90). Management personnel must understand the significance of the research problem and, most importantly, the advantages and solutions achieved by the artifact. Zmud (1997) concludes by advising that presenting result details in a short, concise, and well-articulated manner is an appropriate and effective communication mechanism for both audiences.

Artifacts developed effectively under DSR provide clear contributions regarding the artifact itself, its construction (foundation), and its evaluation (methodology). Hevner et al. (2004) summarize these three types of contributions in Table 5. Next, the concept of fuzzy logic is explained as well as the fuzzy set theory adopted for developing the ISC assessment methodology. Reasons supporting the fuzzy set theory selection are described, including the benefits and advantages a methodology based on FST provide over traditional methodologies.

Table 5. DSR's research contributions

| Contribution | Description |
|---|---|
| Artifact | - The artifact itself (e.g., methodologies, design tools, and prototype systems, etc.), designed to enable solutions to unsolved problems, represents a practical-purpose contribution to the environment. |
| Foundations | - The creation of effective, adequately-evaluated methodologies that also extend and enhance existing methodologies (i.e., foundations) denotes a significant contribution. |
| Methodologies | - The development and use of evaluation methods mentioned earlier (i.e., experimental, analytical, observational, testing, and descriptive) along with their correspondent measures and assessment metrics are crucial contributions of DSR. |

### 3.4 Fuzzy Logic

Based on Zimmermann (2010), the majority of traditional tools for formal modeling, reasoning, and computing are crisp, deterministic, and/or precise in character. Crisp refers to dichotomous, meaning yes or no type answers, rather than a more-or-less type. When dealing with traditional dual logic, for example, statements can be either true or false, nothing else. This implies that the decision of whether an element belongs to a set is unequivocal and has no ambiguities. In other words, parameters within a model are known and there are no doubts about their values or their occurrence. Zimmermann (2010) indicates that (logic) assumptions or beliefs, similar to the above, are not correct in order to describe reality. Zimmermann (2010) further states that the "complete

description of a real system would often require far more detailed data than a human being could ever recognize simultaneously, process, and understand" (p. 317).

According to Klir and Yuan (1995), logic refers to the study of methods for reasoning. Logic can be of type classical and fuzzy, among others. Classical logic relies on the assumption that propositions are either true or false. In fuzzy logic, on the other hand, propositions can be true to some degree, allowing logical reasoning with partially true imprecise statements (Das, 2009). That is, in fuzzy logic, the truth values are no longer restricted to the two values 'true' and 'false', but expressed by the linguistic variables 'true' and 'false' (Zimmermann, 2010).

The subsections below provide a general description of FST and fuzzy reasoning methods, including the Mamdani Max-Min method, followed by the defuzzification process, and the various benefits and advantages of FST over traditional assessment methods. The understanding of these concepts is fundamental to comprehend the fuzzy logic utilized in developing the ISC assessment methodology. To end the section, the data collection method is presented, followed by a summary.

### 3.5 Fuzzy Set Theory

According to Schryen (2010), FST refers to a valuable, uncertainty theory that is useful in the absence of probabilities and in the presence of subjective assessments. The theory has been utilized in many decision-making processes due to its ability to deal with uncertain conditions (Yaakob & Watada, 2009). FST considers uncertainty and constraints to model reality better than traditional theories (Zimmermann, 2010; Schryen, 2010). The idea of FST, as stated by Schryen (2010), is "the extension of the (crisp) membership concept in traditional set theory by providing for a degree with which an

element belongs to a set" (p. 8). Such a degree is specified by a membership function. The degree of truthfulness of propositions –grounded on FST– also allows parameters to be represented with simple linguistic terms (Zimmermann, 2010). The association of linguistic terms with membership functions forms fuzzy sets.

Zadeh (1965) defines fuzzy sets as those sets which have boundaries that are not precise. Moreover, Klir and Yuan (1995) state that a "fuzzy set can be defined mathematically by assigning to each possible individual in the universe of discourse a value representing its grade of membership in the fuzzy set" (p. 4). Such a grade refers to the degree to which that individual, entity, etc., is similar or compatible with the concept represented by the fuzzy set. In other words, those individuals or entities may belong in the fuzzy set, either to a greater or a lesser degree, as indicated by a larger or smaller membership grade (Klir & Yuan, 1995). The membership in a fuzzy set is not a matter of affirmation or denial, right or wrong but rather a matter of a degree (Zadeh, 1965).

Membership grades or functions map elements from any universal set into real numbers within the range 0 - 1. The resulting number represents the degree of membership of elements to particular fuzzy sets, where values closer to one represent higher degrees of membership (Zimmermann, 2010). There are various forms of membership functions and determining the appropriate ones is essential for making FST practically useful (Klir & Yuan, 1995). The most common membership functions used to represent fuzzy numbers are formed by using straight lines. They are: triangular and trapezoidal. Triangular membership functions are usually preferred due to their combination of solid theoretical basis and simplicity (Pedrycz, 1994). Figure 4 shows an example of a triangular fuzzy set to denote AVERAGE as a function of estimated

implementation costs for each ISC. Here, a cost of $25,000 fully belongs to the fuzzy set; therefore, the degree of membership is 1.0. Costs of $20,000 and $30,000 have 0.5 degrees of membership to the fuzzy set, while costs less than $15,000 and greater than $35,000 are not part of the fuzzy set.

Lorterapong (1995) describes a trapezoidal membership function as a function represented by four parameters or characteristic points (i.e., *a*, *b*, *c*, and *d*), where *a* and *d*

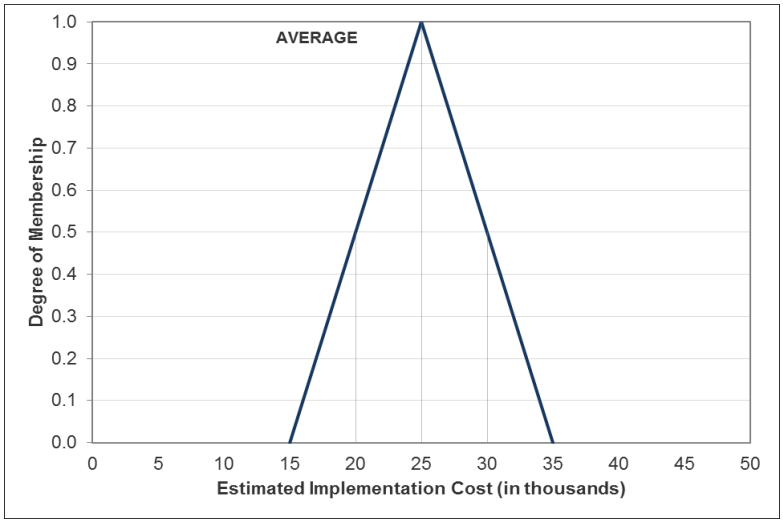



**Figure 4.** Example of a Triangular Fuzzy Set

are the lower and upper bounds, respectively, while *b* represents the lower modal value, and *c* the upper modal value. Figure 5 shows an example of a trapezoidal fuzzy set to denote a MEDIUM classification when measuring the number of applications the particular ISC is expected to protect (i.e., scope). Here, one (1) is the lower bound and four (4) is the upper bound. Two (2) and three (3) in the horizontal axis represent the lower and upper modal values, respectively. In other words, ISC that protect two (2) and three (3) applications fully belong to the fuzzy set shown in Figure 5 and, thus, will have a higher priority of selection; while ISC that do not protect any application (less than one

(1)) and those that protect five (5) applications and more will fall outside of this specific fuzzy set.

There are other situations where more complex functions may be required to represent the degrees of membership of elements in fuzzy sets. Klir and Yuan (1995) discuss direct and indirect methods to form fuzzy sets by gathering and processing responses from subject matter experts, or from literature reviews.

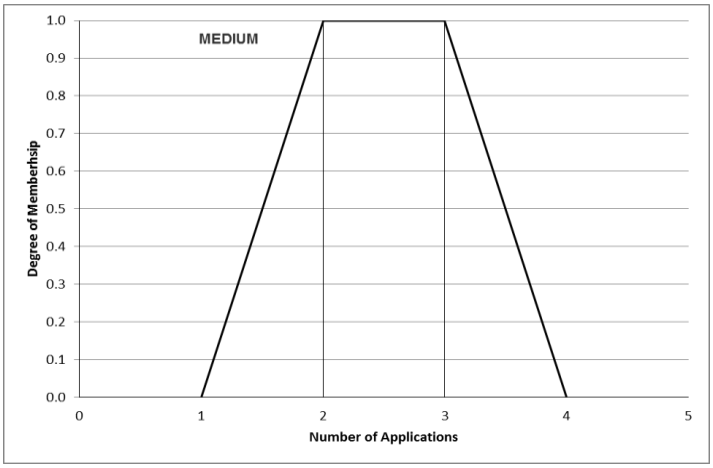



**Figure 5.** Example of a Trapezoidal Fuzzy Set

### 3.6 Fuzzy Reasoning

Based on Das (2009), fuzzy reasoning refers to the process of developing logical inferences from imprecise premises. Such process results from classical logic concepts. In classical logic, a widely used inference rule is the *modus ponens*. The *modus ponens* inference rule states that a conclusion can be inferred given a conditional proposition and a fact. For instance, a classical *modus ponens* inference using the relationship between the value (or score) of a particular ISC, and its level of priority can be expressed as shown in Table 6. Table 6 shows that if the generated value/score of ISC_1 is x

(Proposition 1), and x implies a 'low priority' for an ISC, as defined by the organization based on a specific criteria (Proposition 2), then it can be inferred that ISC_1 has a 'low priority' and, therefore, must not be selected for implementation (Conclusion). Notice that this type of inference structure deals with binary-valued propositions, meaning that the solution set to describe the priority level of a ISC is {0,1} when using the classical *modus ponens*.

Table 6. Classical *Modus Ponens*

| Type of Statement | Statement |
|---|---|
| Proposition 1 | Generated value/score of ISC_1 = x |
| Proposition 2 | 'x' $\Rightarrow$ A low priority ISC as specified by the organization |
| Conclusion | ISC_1 = A low priority ISC |

The classical *modus ponens* just described must be generalized in order to be used for fuzzy reasoning purposes. Such generalization is obtained as follows. First, the generalized version considers degrees of membership of elements to fuzzy sets. Therefore, the solution set to describe the priority level of ISC is expanded from {0,1} to [0,1]. Second, propositions showing completely true implications via the '=>' symbol are replaced with fuzzy rules.

Fuzzy rules are conditional and unqualified propositions implying fuzzy relationships between antecedents and consequences (Klir & Yuan, 1995). This relationship, also known as a fuzzy implication, is not explicit but rather embedded within the proposition and determined for all values of antecedents and consequences (Demicco & Klir, 2004). Fuzzy systems usually involve more than one fuzzy rule. The process of obtaining overall consequences from individual consequences is known as aggregation (Ross, 2010).

Aggregation combines several fuzzy sets to produce a single fuzzy set. Aggregation of rules can be performed:

- conjunctively: rules are jointly satisfied, using connector "AND", producing an aggregate output based on the fuzzy intersection of all individual rule consequences, as well as
- disjunctively: at least one rule needs to be satisfied (trough using connector "OR"), resulting in an aggregate output based on the fuzzy union of all individual rules.

In this dissertation, decisions were made based on the testing of all rules defined within the proposed fuzzy inference system. Therefore, all rules were combined in order to obtain a single fuzzy set. Through the aggregation process, all fuzzy sets that represent the output of every single rule are combined into a single fuzzy set (i.e., determination of whether ISC should or should not be selected).

The third step in generalizing the classical *modus ponens* involves the use of the compositional rule of inference shown in equation (1).

$$\mu_B(y) = \sup_{x \in X} \min [\mu_A(x), R(x, y)] \quad (1)$$

Klir and Yuan (1995) state that equation (1) obtains degree of membership $\mu_B(y)$ for all $y \in Y$ given a fuzzy implication $R$; as well as degree of membership $\mu_A(x)$ given that $R$ is a fuzzy relation on $X$ x $Y$ and $A$ and $B$ are fuzzy sets on $X$ and $Y$, respectively. With the compositional rule of inference, a fuzzy conclusion can be obtained given both, a fuzzy rule and a fuzzy fact. The generalized *modus ponens* form of inference (shown in Table 7) is considered by many as the foundation for various fuzzy reasoning methods presented in the literature (Mizumoto & Zimmermann, 1982).

Table 7. Generalized *Modus Ponens*

| Type of Statement | Statement |
|---|---|
| Fuzzy Rule | If $x$ is $A$, Then $y$ is $B$ |
| Fact | $\mu_A(x)$ |
| Fuzzy Conclusion | $\mu_B(y)$ |

### 3.7 Mamdani Max-Min Fuzzy Reasoning Technique

The fuzzy reasoning technique used in this dissertation was the Mamdani Max-Min (Mamdani) method, which engages the generalized *modus ponens* process just described for each fuzzy rule. This Mamdani method is the most commonly used fuzzy inference technique (Kaur & Kaur, 2012) and it is performed in four steps: (1) Fuzzification of the input variables; (2) Evaluation of rules (inference); (3) Aggregation of the rule outputs (composition); and (4) Defuzzification. The Mamdani method follows the multi-conditional reasoning structure which is illustrated in Table 8.

Based on the Mamdani method, the fuzzy implication (required by the compositional rule of inference) equals the truth value of the antecedent. In other words, and based on

Table 8. Multi-conditional Reasoning Structure

| Type of Statement | Statement |
|---|---|
| Rule 1 | If $x$ is $A_1$, then $y$ is $B_1$ |
| Rule 2 | If $x$ is $A_2$, then $y$ is $B_2$ |
| … | … |
| Rule $n$ | If $x$ is $A_n$, then $y$ is $B_n$ |
| Fact | $\mu_A(x)$ |
| Conclusion | $\mu_B(y)$ |

Otero and Otero (2011), the fuzzy implication for singleton fuzzy rules equals the degree of membership of the only statement in the antecedent (Figure 6A). For non-singleton fuzzy rules and based on operator ‘AND’, the fuzzy implication is computed as the

intersection or conjunction of the statements in the antecedent via the minimum logical operation shown in equation (2) (Figure 6B).

$$\mu_{A\cap B}(x) = \min [\mu_A(x), \mu_B(x)] \quad (2)$$

Equation (2) returns the smallest element where *A* and *B* are limited to the range (0, 1). Fuzzy operator 'OR', on the other hand, is known as the fuzzy union or disjunction, returning the maximum elements where again *A* and *B* are limited to the range (0, 1). It is denoted by equation (3), where *A* and *B* are two given fuzzy sets with memberships functions $\mu_A(x)$ and $\mu_B(x)$.

$$\mu_{A\cup B}(x) = \max [\mu_A(x), \mu_B(x)] \quad (3)$$

An antecedent with a truth value greater than zero automatically implies that its consequence also has a truth value greater than zero. In fuzzy reasoning terms, a true antecedent causes a rule to fire. The fired rules are then combined into fuzzy sets which are used to make final inferences (Figure 6C). Fired rules will be combined according to each criteria or fuzzy set evaluated. In evaluating ISC, the methodology will require the creation of a fuzzy set for each criteria evaluated. Evaluation criteria in this study include estimated implementation costs, scope, compliance, and risks. Therefore, there were four fuzzy sets created for cost, scope, compliance, and risks used to assess and determine ultimate ISC selection. Each criteria have its own set of fuzzy or inference rules defined to assist with the evaluation. Upon the result of truth values from antecedents, fired rules are aggregated per criteria, and utilized for final ISC selection inference.

### 3.8 Mamdani and Other Fuzzy Reasoning Methods

Other very common fuzzy implication or inference mechanism methods include the Sugeno-Type Fuzzy Inference (also known as Takagi-Sugeno method) and the Larsen Product Implication, both described in Table 9.

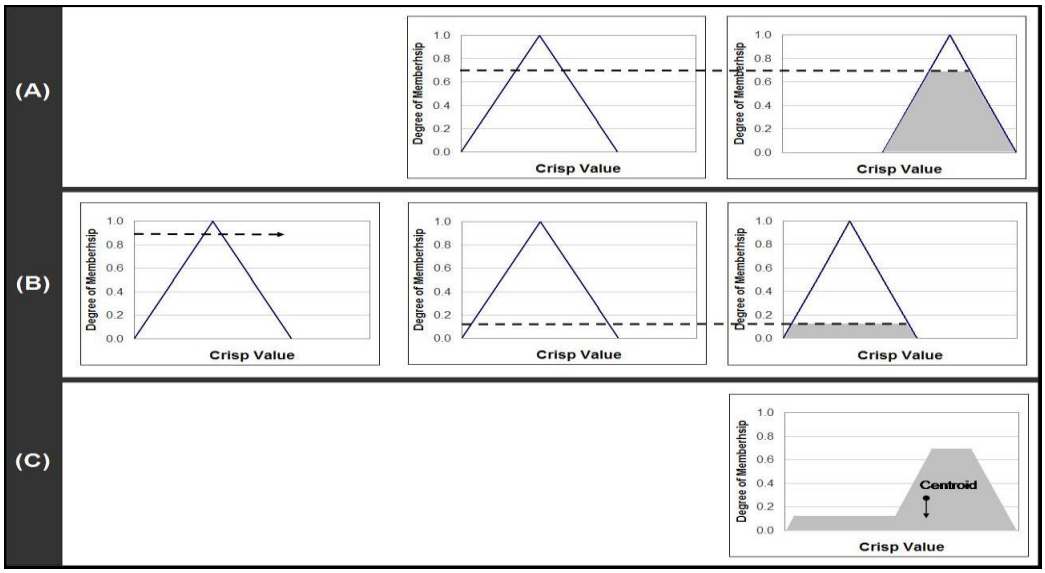



**Figure 6.** Mamdani Max-Min Inference

When compared to the Mamdani approach, Kaur and Kaur (2012) state that the Sugeno-Type Fuzzy Inference method (1) works well with optimization and adaptive techniques, which makes it very attractive in control problems; (2) has enhanced processing time over the Mamdani's defuzzification process; (3) is computationally efficient since it

Table 9. Common Fuzzy Reasoning Methods

| Method | Description |
|---|---|
| Sugeno-Type Fuzzy Inference | Similar to the Mamdani method in the first two parts of the fuzzy inference process (i.e., fuzzifying the inputs and rules evaluation). Nonetheless, its output membership functions are either linear or constant. That is, instead of a fuzzy set (or defuzzification) as used by Mamdani, Sugeno uses a mathematical function (weighted average) of the input variable to compute the crisp output (Kaur & Kaur, 2012). |
| Larsen Product Implication | Larsen uses the arithmetic product operation between the two membership functions as a fuzzy implication in the universe of discourses (Larsen, 1980). |

works with linear techniques; and (4) may guarantee continuity of the output surface and is well-suited to mathematical analysis. Nevertheless, the Mamdani approach is more intuitive and has a widespread of acceptance. The major disadvantage of the Sugeno method is that it is not well suited to human input when compared to the Mamdani approach. Moreover, the expressive power and interpretability of Mamdani output is lost in Sugeno since its consequents or outputs are not fuzzy, but linear or constant in nature.

The Larsen product implication method is somewhat similar to the Mamdani method described above, but it uses the arithmetic product operation (i.e., multiplication) between the two membership functions as a fuzzy implication in the universe of discourses (Larsen, 1980). This way, the overall antecedent of the fuzzy rule is the maximum of the two fuzzy propositions of the antecedent. Mamdani, on the other hand, uses fuzzy operators 'AND' and 'OR' to obtain a single number that represents the result of the antecedent evaluation. The operator 'AND' evaluates the intersection or conjunction of the rule antecedents, while 'OR' assesses the union or disjunction of the rule antecedents. The Larsen product implication, however, becomes computationally difficult as more and more rules are added to the fuzzy evaluation system (Larsen, 1980). The Mamdani approach may also entail a substantial computational burden (i.e., increase in computing time) as the number of rules grows, however, the precision of the system also increase with the increment in fuzzy rules (Bhoyar & Kakde, 2009).

The Mamdani method was chosen for this dissertation because, when producing output for decision-making, it does so by providing fuzzy, non-linear conclusions obtained given both, fuzzy rules and fuzzy facts. Given the high subjectivity identified in current evaluation methods from the literature when selecting ISC in organizations,

Mamdani offers advantages when providing for mathematical convenience due to its simplicity and low computational complexity, high degree of accuracy when evaluating imprecision information, and ease of implementation and testing. In Sugeno, the output produced is not fuzzy-based (as Sugeno has no output membership functions), but restricted to constant or linear values. In other words, outputs in Sugeno are limited, subject to the range 0-1 (Kaur & Kaur, 2012), which makes the approach not suitable when handling imprecise criteria as required by this dissertation.

Another critical advantage of using a rule-based approach such as Mamdani is that processing for all received inputs, via fuzzy 'if-then' rules, is strictly human based. This approach can be expressed in simple language words using the logic a human would use to perform the tasks. Cox (2005) supports the aforementioned by stating that a Mamdani's fuzzy rule-based system derives its 'expertise' (rule induction process) from subject matter experts. The rules represent nonprocedural statements of knowledge in the form of 'if-then' sentences. The rules also reference local variables that, in turn, reference fuzzy sets which ultimately define control regions over the variables' domain. Cox (2005) further states that the framework of a rule-based approach is "relatively uncomplicated" (p.100).

As evidenced, the Mamdani approach represents a suitable method for performing an effective evaluation of ISC in organizations. Such fuzzy reasoning technique offers robustness, as its defined rules tolerate imprecise measurements and component variations, and easy adaptation in terms tuning fuzzy rules as it becomes necessary (Salmasi, 2007). According to Kaur and Kaur (2012), its intuitiveness, human-like manner for capturing expert knowledge, expressive power and interpretability of its fuzzy

output, as well as its widely use, particularly, in decision support applications, made the Mamdani method the appropriate reasoning technique for this dissertation.

### 3.9 Defuzzification

Defuzzification converts conclusions from fuzzy sets into a real number, or a single crisp value (Yager, 1996). Ross (2010) also defines the defuzzification process as the conversion of a fuzzy quantity to a precise quantity, represented by the logical union of two or more fuzzy membership functions defined on the universe of discourse of the output variable. In other words, the purpose of defuzzification is to find one single crisp value that summarizes the fuzzy set. There are several methods available for defuzzification; among the most common are the center of gravity approach (i.e., centroid) and the weighted average method (Ross, 2010).

The centroid method is the most prevalent and intuitively appealing defuzzification technique. This method takes the center of gravity (COG) and uses integrals to calculate the area of a combination of fuzzy sets. Equation (4) describes algebraic expression for this method, where $\mu_A$ are the degrees of membership

$$COG = \frac{\int_a^b \mu_A(x)\, x\, dx}{\int_a^b \mu_A(x)\, dx} \tag{4}$$

The calculation of the center of gravity is simplified if a finite universe of discourse and thus a discrete membership function is considered.

$$COG = \frac{\sum_{i=1}^{n} \alpha_i \mu_i}{\sum_{i=1}^{n} \alpha_i A_i} \tag{5}$$

In equation (5), $\mu_i$ is the value of the membership function of the fuzzy set rule *i*, $A_i$ is the corresponding area and $\alpha_i$ is the degree that the rule *i* is fired (between 0 and 1). Figure 6C illustrates the center of gravity or centroid of a fuzzy set.

Other methods, such as the weighted average method (shown in equation 6), are reliable, less complicated, less time consuming, and also accurate to approximate the center of gravity (Genske & Heinrich, 2009). The weighted average defuzzification method, based on peak values for every fuzzy set, calculates weighted sums of the peak values. Based on those weight values and the degree of membership for fuzzy outputs, crisp values of the output are determined using the following formula, where $\mu i$ is the

$$Z_0 = \frac{\sum \mu(x)_i \times W_i}{\sum \mu(x)_i} \tag{6}$$

degree of membership in output singleton *i*, and *Wi* is the fuzzy output weight value for the output singleton *i* (Ross, Hassanein, & Ali, 2010). The weighted average method has also been frequently used in cases similar to this dissertation (Otero & Otero, 2011). Nonetheless, the weighted average method is usually restricted to symmetrical output membership functions, a limitation identified by Ross (2010). In this dissertation, the center of gravity approach or centroid method was employed. Figure 6C shows an example of the estimated center of gravity of a fuzzy set converted using the center of gravity approach from two fired fuzzy rules. Figure 7 depicts, at an overall level, the steps just described within a fuzzy inference system.

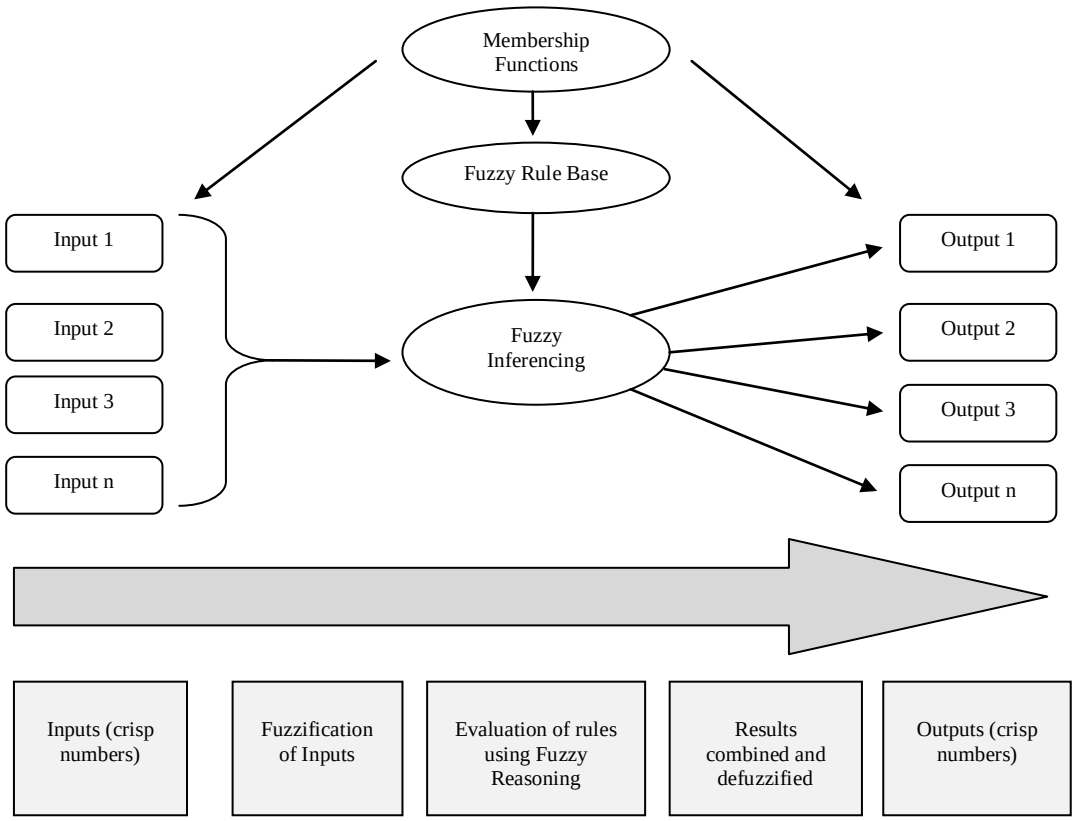



**Figure 7.** Fuzzy Inference System

### 3.10 Benefits and Advantages of FST over Traditional Methods

Based on the above, and as supported by Zimmermann (2010), a FST-based framework: (1) provides a natural, effective way of handling problems in which the source of imprecision is the absence of sharply defined criteria; (2) offers a strict mathematical methodology that can precisely and rigorously examine vague conceptual phenomena; (3) has been used as a modeling, problem solving, and data mining tool, and has proven superior to existing methods, as well as attractive to enhance classical approaches; (4) relaxes classical and/or traditional assumptions through fuzzy reasoning; and (5) suggests opportunities to improve existing methodologies and approaches. Kaur

and Kaur (2012) further stress the flexibility of the fuzzy approach, particularly, when adding more variables to a problem, as it would only require writing new rules or editing the existing ones. The above translates into a lesser amount of effort than rewriting an entire algorithm.

Klir and Yuan (1995) state that since FST deals with uncertainty, it is a great utility also considered essential to science. FST assists in understanding the phenomenon of reality (be it natural or man-made) via: (1) performing adequate predictions or retrodictions; (2) learning about controlling the phenomenon; and (3) utilizing such capabilities for various other ends. Furthermore, a FST-based approach leads to more detailed and thorough assessments (Otero & Otero, 2011), while appropriately modeling human decisions, which are imprecise in nature (Petrovic-Lazarevic, 2001).

### 3.11 Data Collection Method and Rationale for its Adoption

To create the FST-based ISC assessment artifact, specific data from the organization needed to be collected. The data collection method adopted for this study involved survey approach. A questionnaire was provided to key information security management personnel within the organization, such as, the Information Security Manager, Information Security Director, or the Chief Information Security Officer, as applicable.

The survey/questionnaire approach is used when a series of questions are posed to willing participants and their responses are summarized with percentages, frequency counts, and/or more sophisticated statistical indexes (Leedy & Ormrod, 2001). Then, inferences about particular populations are drawn from the responses of the sample. Surveys are a common approach used with more or less sophistication in many areas of

human activities. Survey research typically employs online assessments, written questionnaires, face-to-face interviews, or telephone interviews (Leedy & Ormrod, 2001).

Skulmoski, Hartman, and Krahn (2007) state that online technologies facilitate the administration and management of surveys, particularly, questionnaires, as they allow control by the researcher. Online questionnaires have extensively been used in the literature to collect individuals' data (Cabaniss, 2001; Richards, 2000; Schmidt, 1995). Administration of questionnaires was conducted through e-mail which provides many advantages to both, researcher and participants (Skulmoski et al., 2007), as e-mails can speed up the questionnaires' turnaround time.

Questionnaires also examine the level of agreement or disagreement of participants (Sekaran, 2003). Additional support for using surveys or questionnaires is provided by Leedy and Ormrod (2001) when stating that survey approach looks more closely at phenomena of the moment and, therefore, captures responses/feedback from a specific moment in time.

To expand on the above, requests for participation were made for organizations meeting the following requirements:

- Industry: Schools, Universities, and Not-for-profit
- Location: Puerto Rico
- Size: Small-to-Medium
- Convenience and Availability

A critical part of the scope of this dissertation involved the information systems (i.e., applications) to be in scope. The systems and applications where ISC were evaluated comprised only financial applications. All other applications and/or information systems

within organizations (e.g., applications, databases, operating systems, networks in place for operational / non-financial purposes, etc.) were not included in this dissertation.

The target audience comprised information security management personnel. Due to their knowledge and experience, the target audience reflected an accurate representation of the population, allowing for results to be generalizable and, thus, consistently applied to other populations with the same characteristics in different settings (Salkind, 2009).

Data collected from participants will be maintained and available only for investigation and analysis purposes. Moreover, to increase confidence, the survey participants were assured that no personal information will be attached nor disclosed to their responses, and that the data collected will be strictly for research purposes. To attract participants and encourage their involvement in the study, the study's research results will be made available to interested participants, as suggested by Okoli and Pawlowski (2004).

### 3.12 Summary

This Chapter provided an overview of the research methodology as well as the specific research method that was used. Chapter three also explained the fuzzy set theory adopted for developing the ISC assessment methodology, including reasons supporting its selection, as well as the underlying assumptions. Benefits and advantages of a FST-based methodology over traditional methodologies were also mentioned. Moreover, Chapter three presented the data collection method used and the rationale for its adoption.

# Chapter 4

# Results

## 4. Introduction

The purpose of this chapter is to present and discuss the results of this dissertation. Specifically, a description of the data collection process is provided, followed by an explanation of the development of the FST-based artifact, including descriptions of the Fuzzy Logic Toolbox of MATLAB editors and viewers used. Findings and results are also discussed, as well as detailed evaluations of the artifact developed against (1) traditional ISC assessment methodologies, and (2) the organization's already implemented ISC, to determine whether the proposed hypotheses described in sub-section "Research Questions and Hypotheses" have been supported. Lastly, a summary is presented to close the chapter.

Data for this research were collected via a questionnaire sent through email (see Appendix A). As stated earlier, e-mails can speed up the questionnaires' turnaround time and look more closely at phenomena of the moment, capturing responses and feedback from a specific moment in time. Given that the ISC and Security Areas included in the questionnaire were adopted from the ISO/IEC 27002 (2005) Baseline Manual or Best Practice Framework, which is well known and a widely accepted model, the validity of the questionnaire was acceptable. Additionally, the content of the questionnaire was pre-tested as well as edited, as necessary, by three subject matter experts for semantic and syntactic checking purposes, as suggested by Emory and Cooper (1991). The three experts have around 15-20 years of experience and have held Management positions

within global, also known as Big Four, accounting and audit firms. They have also provided numerous auditing and consulting services to small-to-medium size type organizations within the schools, universities, and non-profit industry, among others. The experts' experience also includes working for private industries, as well as for information systems and technology audit departments.

The questionnaire was emailed to the Information Security Manager (ISM) of a small-to-medium size organization within the industry of schools, universities, and not-for-profits. The specific organization is a University located in Puerto Rico that offers associate, baccalaureate, masters, and doctoral degrees in arts, humanities, natural and social sciences, as well as in professional areas such as business, education, nursing, law, and medical technology. Currently, there are approximately 15,000 students attending.

In regards to IT and related support activities, the organization's approach is centralized. That is, the organization's computer processing is performed by its IT Department, which is the sole provider of technology and telecommunications for the various departments. Furthermore, the IT Department provides data processing and end-user support for the organization's systems and applications, including training and documentation of application system controls and procedures. The IT Department's organizational structure consists of approximately 30 staff, under the direction of an IT Executive Director. For purposes of this dissertation, the organization specifically requested to remain anonymous and not make the results publicly available. The anonymous request just mentioned is consistent with various studies from the literature such as Bowman (2009), as well as Wang, Xu, Chan, and Chen (2002). In Bowman (2009), the microeconomic theory was applied to the problem of calculating the

economic value of volunteers to nonprofit organizations. Case study and survey analysis performed in an anonymous Australian organization supported the investigation. In another study, critical success factors of a web-based training system within an anonymous organization were raised and evaluated via survey analysis (Wang et al., 2002). In a further study, both the perceived organizational support for safety and the perceived coworker support for safety were evaluated as predictors for employee safety voice, using survey analysis on urban bus drivers from a United Kingdom's anonymous organization (Tucker, Chmiel, Turner, Hershcovis, & Stride, 2008).

Upon receipt of the questionnaire and as planned, the ISM started by identifying the ISC already in place at the organization that protect financial-related applications (Step 1). All other applications and/or information systems within the organization (e.g., applications, databases, operating systems, networks, etc.) in place for operational or non-financial purposes were out of scope for purposes of this dissertation. In other words, the ISM only identified the ISC that were implemented to secure financial-related applications. The purpose of identifying the ISC already in place is to compare them with the ones generated by the newly-developed methodology and evaluate, consistent with Hypothesis 2, whether the new set of ISC enhances information security in the organization. The ISC were selected from an all-inclusive list of ISC from the ISO/IEC 27002 best practice framework.

Following identification of the ISC currently implemented, the ISM ranked, in order of relevance, the 11 information security areas found in the ISO/IEC 27002 best practice framework (Step 2). As instructed and for purposes of this dissertation, the ISM identified the first three ranked information security areas. These were: Access Control,

Compliance, and Human Resources Security. As mentioned earlier, a significant advantage of the FST-methodology built herein is that it can accept and, thus, evaluate unlimited information security areas (not only the three included in this dissertation).

For each ISC within the three ranked information security areas, and in order to start the assessment process (Step 3), the ISM provided specific data related to literature-supported criteria (i.e., EIC, Scope, Compliance, and Risks). That is, for each ISC, the ISM entered data related to EIC, Scope, Compliance, and Risks. For instance, for one ISC within the Access Control information security area, the ISM entered the following:

- EIC - $16,000;
- Number of systems/applications protected by ISC (Scope) - 2;
- Extent to which the ISC complies with required, external laws and regulations (Compliance) - 20%; and
- Extent to which the ISC addresses information security risks (Risks) - 15%.

With the specific information provided by the ISM related to each ISC within the three ranked information security areas, the FST-based artifact was ready to be developed using the Fuzzy Logic Toolbox of MATLAB.

**4.1 Artifact Development**

According to the DSR Guidelines in Hevner et al.'s (2004), and correspondent Process Steps from Vaishnavi and Kuechler's (2004) General Methodology of DSR, and consistent with Process Step 3: Development from Chapter three, the following explains how the FST-based artifact was developed.

Hevner et al. (2004) state that the ultimate result of DSR is a purposeful IT artifact developed to provide a solution to a significant organizational problem. In the context of

this dissertation, the artifact built refers to a FST-based ISC assessment methodology. FST allows for prioritization of ISC within information security areas (identified by an organization as relevant) by fusing their respective assessment values into a single, quantified measure using the Mamdani Max-Min fuzzy reasoning technique. This provides organizations with a measurement of relevance for each ISC based strictly on organizations' specific criteria (i.e., EIC, Scope, Compliance, and Risks), including goals, objectives, and restrictions. The derived relevance measurement is used as the main metric for evaluating and ultimately selecting ISC.

The artifact was built using the Fuzzy Logic Toolbox of MATLAB ("toolbox"). The toolbox is a tool for solving problems with fuzzy logic. The toolbox refers to a collection of functions built on the MATLAB computing environment that provides tools and technologies to create and modify fuzzy inference systems (FIS) within the framework of MATLAB. The toolbox provides several interactive tools that allow access to many of the functions through a graphical user interface (also known as "GUI"). These GUI-based tools set an environment for FIS design, analysis, and implementation. A significant advantage of the toolbox is that it links most of human reasoning and concept formation to fuzzy rules. That is, the toolbox amplifies the power of human reasoning through providing a systematic framework for computing with fuzzy rules.

The toolbox comes with five GUI editors and viewers defined to build, edit, and view FIS. The FIS interprets the values in the input vector and, based on user-defined rules, assigns values to the output vector. Using the editors and viewers within the toolbox, a rules-set is built, membership functions are defined, and FIS behaviors get analyzed. Table 10 lists and describes the editors and viewers just mentioned.

Table 10. Description of Toolbox's Editors and Viewers

| Editors and Viewers | Description |
|---|---|
| FIS Editor | Displays general information about a FIS. It is within this editor that inputs are defined and named, as well as outputs. This editor also displays information such as the name of the FIS, type of fuzzy reasoning that is used (i.e., Mamdani), and defuzzification method (i.e., centroid), among other information. |
| Membership Function Editor | Allows for editing the various membership functions associated with the input and output variables of the FIS. It is within this editor that membership functions that describe input and output variables are either created or edited. |
| Rule Editor | Displays and allows for editing the various fuzzy rules using one of three formats: full English-like syntax (verbose), concise symbolic notation, or an indexed notation. It is within this editor that rule statements that define the behavior of the system (also known as if-then rules) get created and modified. |
| Rule Viewer | Displays detailed behavior of a FIS based on the specific rules defined; also, examines the effect and behavior of modifying input variables. |
| Surface Viewer | Generates a three-dimensional surface resulting from inputs in relation to the output. The dependency of one output on any two inputs or one input is represented by the output surface map. |

Figure 8 illustrates a summary of the Toolbox editors and viewers just described that were used to develop the artifact. Specifically, Figure 8 shows the FIS Editor (top center), Membership Function Editor (top left), Rule Editor (top right), Rule Viewer (bottom left), and Surface Viewer (bottom right).

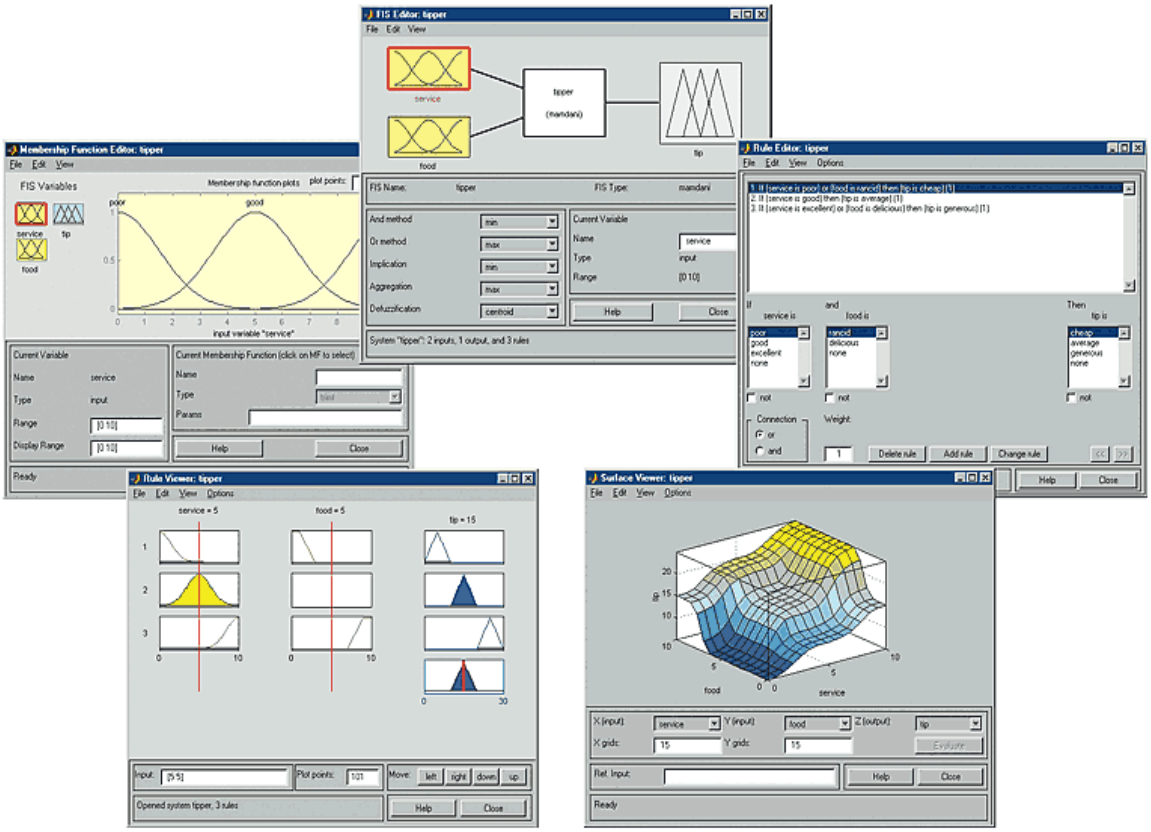


**Figure 8.** Toolbox Editors and Viewers

Following are snapshots, descriptions, and explanations of the editors and viewers used specifically for building the Fuzzy-based artifact.

4.1.1 FIS Editor

For purposes of the FST-based artifact being created, there are four fuzzy input variables defined (also known as linguistic terms), each constituting a specific, literature-supported evaluation criteria (i.e., Estimated Implementation Costs (EIC), Scope, Compliance, and Risks). Refer to Figure 9. Estimated Implementation Costs for purposes of this assessment consider capital or operating expenditures on hardware, software, and personnel (Gordon & Loeb, 2006). Estimated Implementation Costs represent a critical

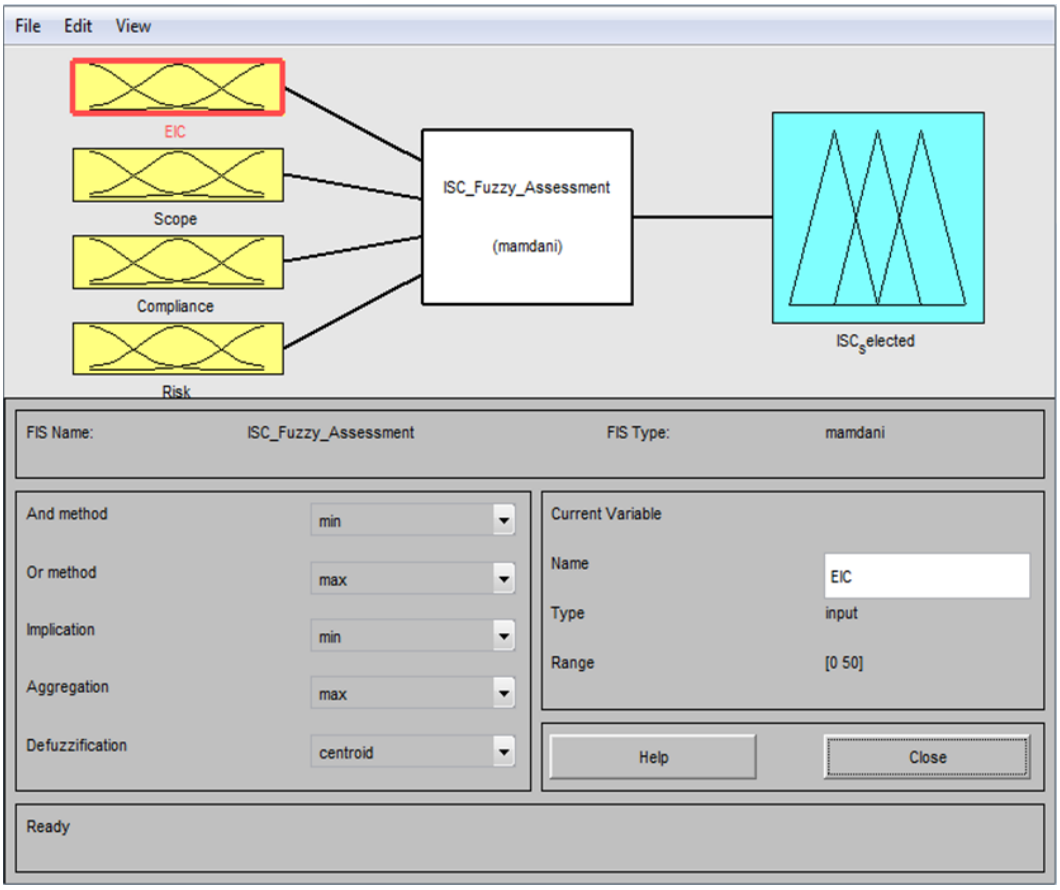



**Figure 9.** FIS Editor

factor that must be closely evaluated and monitored by management before selecting and implementing ISC (ISO/IEC 27002, 2005). Ou Yang et al. (2011) support this claim by stating that "managers should consider the related costs and resources when they implement the controls…" (p. 18). Significant implementation costs will likely preclude the selection of ISC. The second evaluation factor, Scope, assesses the impact of the ISC on the organization. ISC that provide security of information in multiple systems and/or applications rather than on a minimal number of systems and/or applications will have a higher priority of selection (Otero et al., 2012a; Ejnioui et al., 2012; Otero et al., 2010). The third factor to evaluate when determining selection of ISC is Compliance with rules,

laws, regulations, policies and procedures, etc. According to the ISO/IEC 27002 (2005), ISC assist organizations in complying with legal, statutory, regulatory, and contractual requirements, as well as with organizations' established policies, principles, standards, and/or objectives (collectively referred to as "policies"). Compliance, as defined by Saint-Germain (2005), includes ensuring "that all laws and regulations are respected and that existing policies comply with the security policy in order to ensure that the objectives laid out by senior management are met" (p. 62). Saint-Germain (2005) also states that the lack of security compliance, perhaps by selecting and implementing the wrong set of ISC, can translate into business losses and, even worst, severe civil and criminal penalties, which can include fines and prison sentences. The higher the policies the ISC complies with, the higher its chances for selection. The last evaluation factor for purposes of this dissertation involves the number of Risks that are addressed from implementing ISC. Per NIST SP 800-30, risks are mitigated and/or reduced to acceptable levels through implementing the necessary controls (i.e., ISC). The higher the number of risks the ISC addresses, mitigates, or reduces; the higher its possibility for selection (Gerber & von Solms, 2008). The output variable used and evaluated within this dissertation was named ISC_Selected.

#### 4.1.2 Membership Function Editor

Membership functions were created for each particular input considering the literature reviewed as well as input from field experts. When evaluating EIC, for instance, the fuzzy sets or alternatives for evaluation defined within this dissertation (i.e., low, average, and high) determine the degrees of membership for the crisp or actual data values obtained. The fuzzy set definitions of low, average, and high used were supported

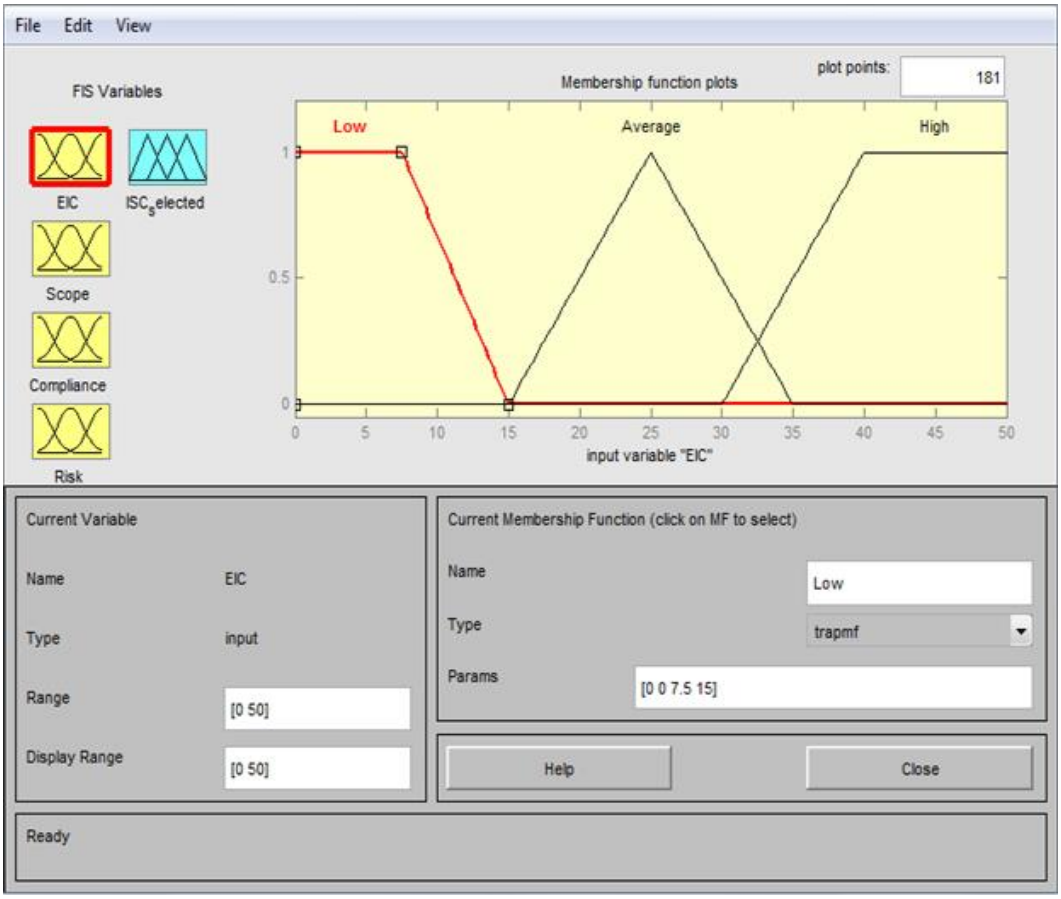



**Figure 10.** Membership Function Editor for EIC

by and validated with decision-makers within the organization. The fuzzy set for Average is depicted in a common triangular shape form in Figure 10 (values are expressed in thousands of dollars). As illustrated in Figure 10, the average estimated implementation cost for an ISC is defined in the range of $15,000 and $35,000. Additionally, a cost of $25,000 fully belongs to the fuzzy set; therefore, the degree of membership, or fuzzified input, is 1.0. EIC's of $20,000 and $30,000 have 0.5 degrees of membership to the fuzzy set, while EIC's less than $15,000 and greater than $35,000 are not part of the fuzzy set.

Table 11 illustrates the inputs and output that have been defined as relevant for the FST-based artifact along with their corresponding ranges and membership functions.

As stated earlier, the input and output variables defined (also known as linguistic terms), constitute a specific, literature-supported evaluation criteria (refer to Figure 9). The range values utilized on each of the fuzzy sets resulted from phone calls and meetings held with decision-makers within the organization, particularly with the ISM. The range values used, according to Management, are considered standard when evaluating information security-related controls and procedures for potential implementation, as well as represent current practices within the industry. A similar approach was followed to support and validate the fuzzy set definitions (e.g., low, average, and high, etc.) specific to the inputs and output used in this dissertation.

Table 11. FST-based FIS Inputs and Output

| **Inputs** | **Output** |
|---|---|
| Estimated Implementation Cost (EIC)<br>Range: $0 - $50,000<br>Membership Functions: 3<br>  Low<br>  Average<br>  High<br><br>Scope<br>Range: 0 - 5<br>Membership Functions: 3<br>  Low<br>  Medium<br>  High<br><br>Compliance<br>Range: 0 - 100%<br>Membership Functions: 2<br>  Not-Comply<br>  Comply<br><br>Risk<br>Range: 0 - 100%<br>Membership Functions: 2<br>  No<br>  Yes | ISC Selected<br>Range: 0 - 10<br>Membership Functions: 2<br>  No<br>  Yes |

Table 12 shows the membership function values for input EIC, while Figure 11 shows the graph of all membership functions within input EIC.

Table 12. Membership Functions of the EIC Input (values are expressed in thousands of dollars)

| Fuzzy Set | Membership Function | Values |
|---|---|---|
| Low | Trapezoidal | 0, 0, 7.5, 15 |
| Average | Triangular | 15, 25, 35 |
| High | Trapezoidal | 30, 40, 50, 50 |

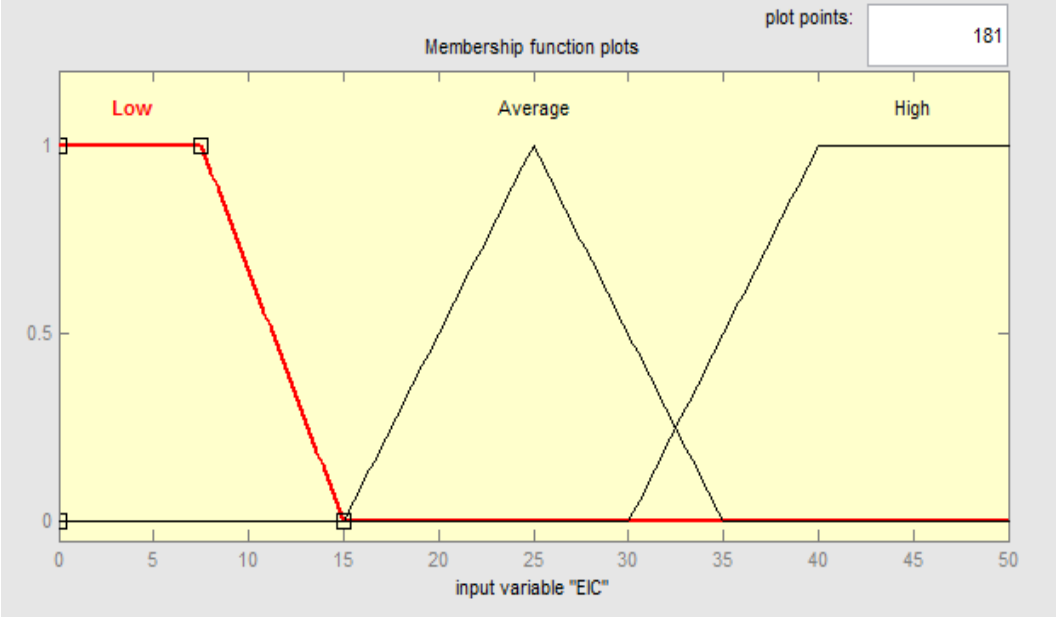



**Figure 11.** Graph of Membership Functions within the EIC Input

Table 13 shows the membership function values for input Scope, while Figure 12 shows the graph of all membership functions within input Scope.

Table 13. Membership Functions of the Scope Input

| Fuzzy Set | Membership Function | Values |
|---|---|---|
| Low | Trapezoidal | 0, 0, 1, 2 |
| Medium | Trapezoidal | 1, 2, 3, 4 |
| High | Trapezoidal | 2, 4, 5, 5 |

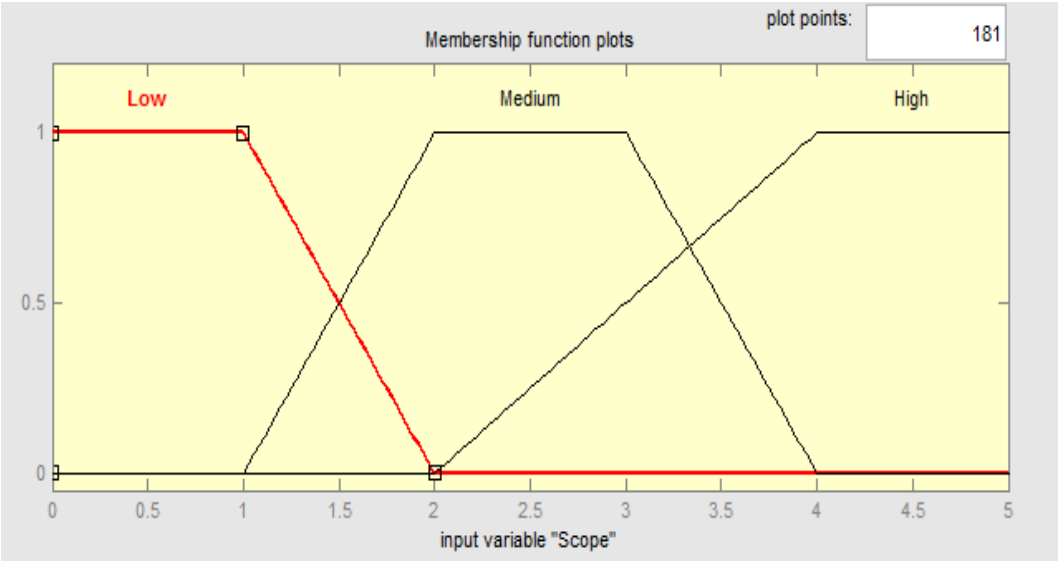



**Figure 12.** Graph of Membership Functions within the Scope Input

Table 14 shows the membership function values for input Compliance, while Figure 13 shows the graph of all membership functions within input Compliance.

Table 14. Membership Functions of the Compliance Input

| Fuzzy Set | Membership Function | Values |
|---|---|---|
| Not-Comply | Trapezoidal | 0, 0, 60, 90 |
| Comply | Trapezoidal | 85, 90, 100, 100 |

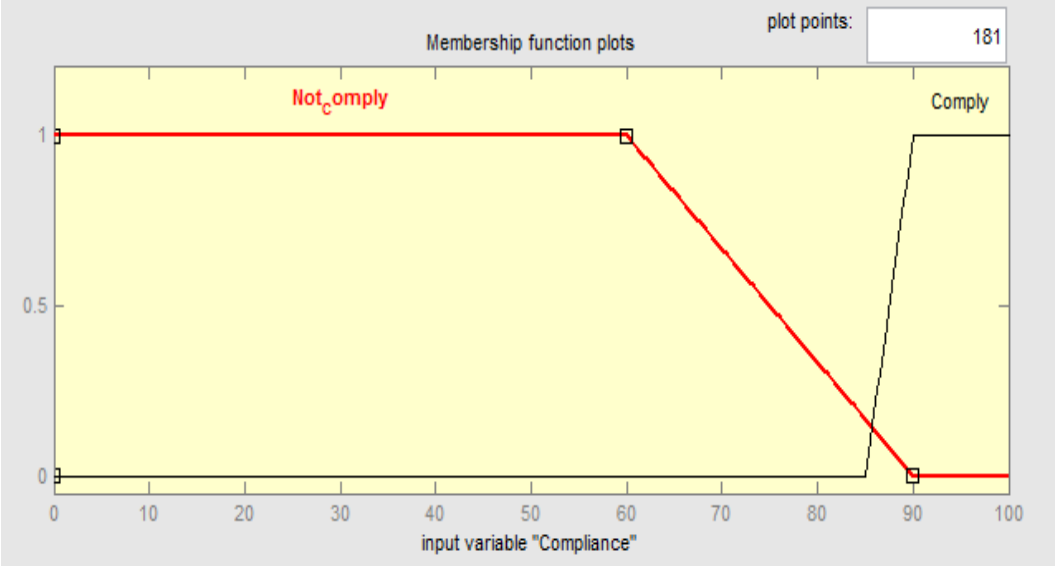



**Figure 13.** Graph of Membership Functions within the Compliance Input

Table 15 shows the membership function values for input Risk, while Figure 14 shows the graph of all membership functions within input Risk.

Table 15. Membership Functions of the Risk Input

| Fuzzy Set | Membership Function | Values |
|---|---|---|
| No | Trapezoidal | 0, 0, 50, 80 |
| Yes | Trapezoidal | 75, 85, 100, 100 |

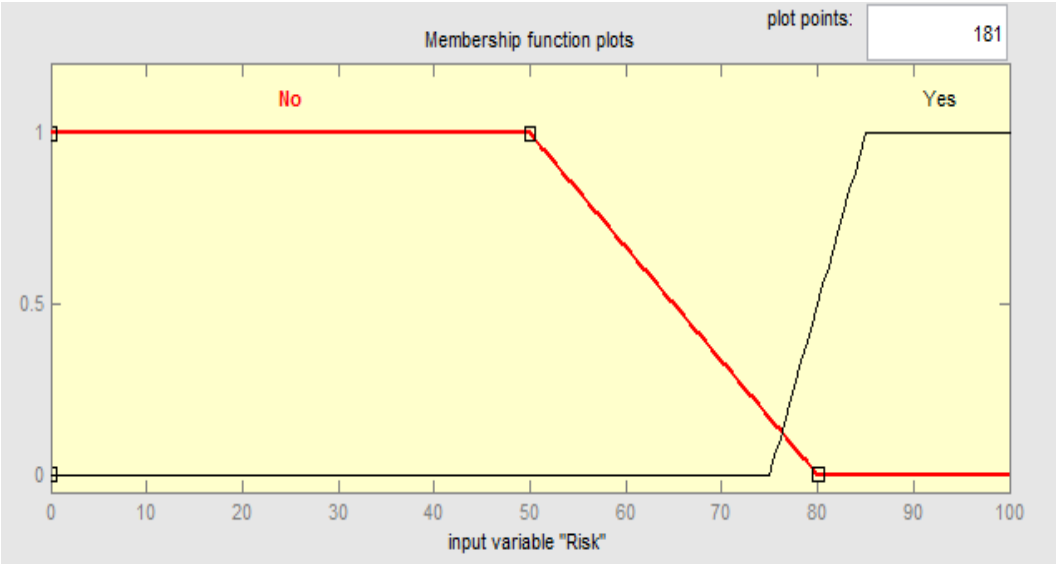



**Figure 14.** Graph of Membership Functions within the Risk Input

Table 16 shows the membership function values for output ISC Selected, while Figure 15 shows the graph of all membership functions within output ISC Selected.

Table 16. Membership Functions of the ISC_Selected Output

| Fuzzy Set | Membership Function | Values |
|---|---|---|
| No | Trapezoidal | 0, 0, 6, 8 |
| Yes | Trapezoidal | 8, 9, 10, 10 |

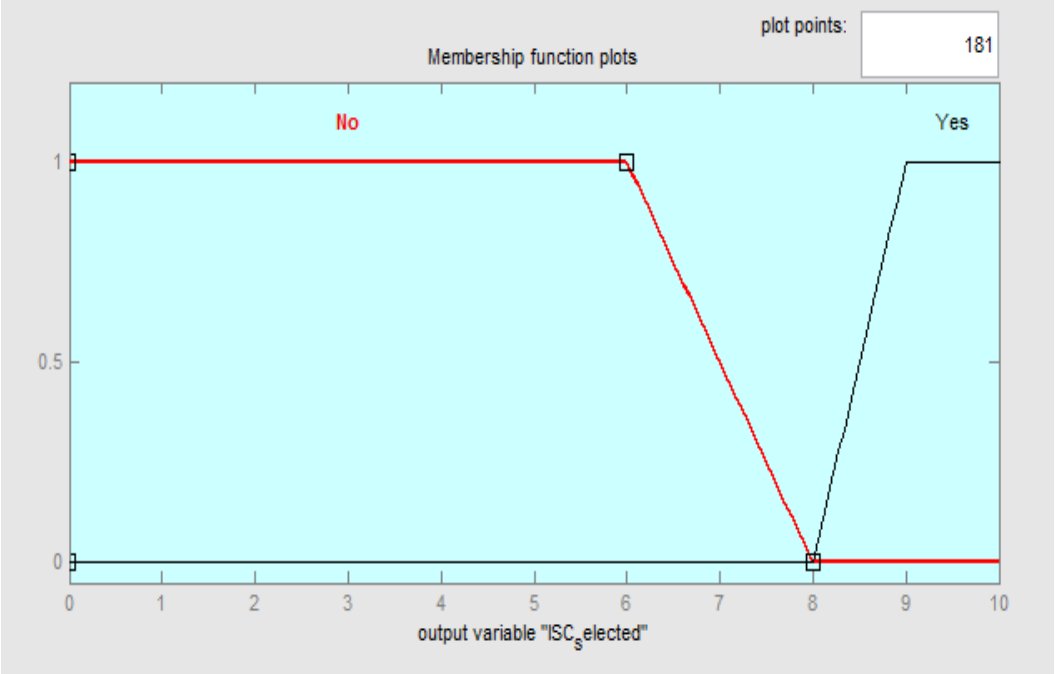



**Figure 15.** Graph of Membership Functions within the ISC_Selected Output

### 4.1.3 Rule Editor

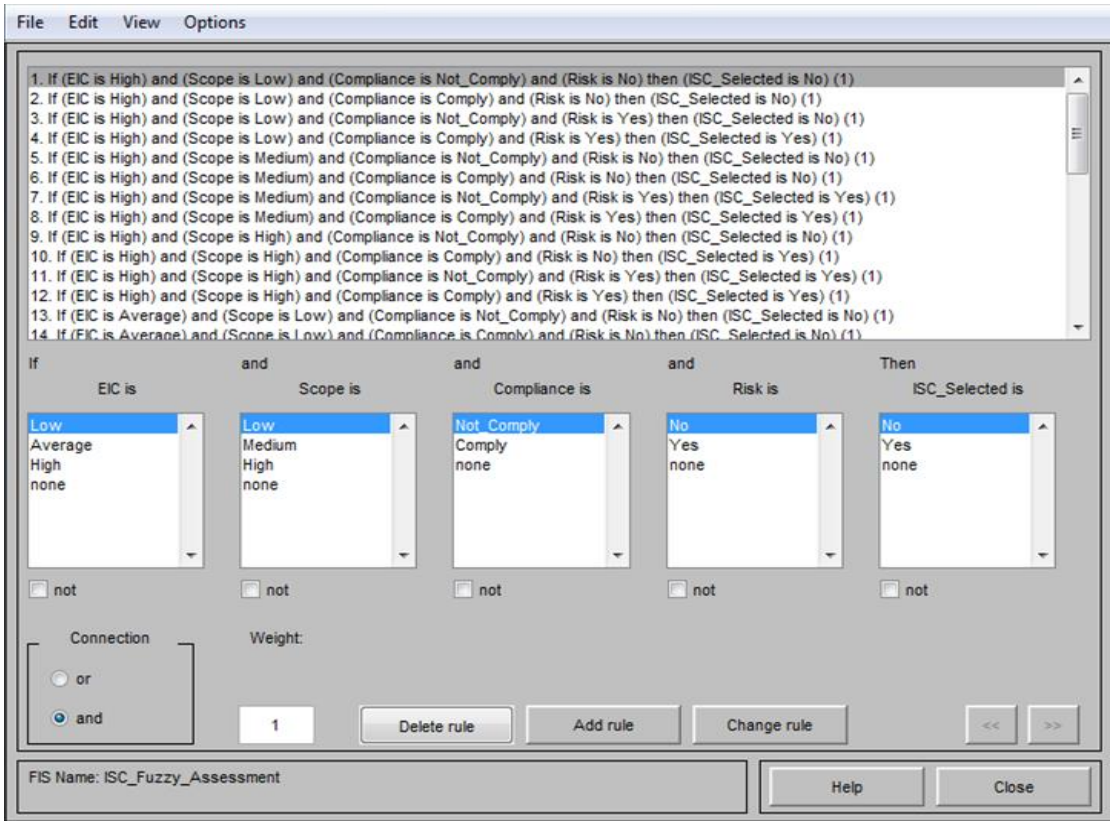



**Figure 16.** Rule Editor

Within the rule editor (see Figure 16), fuzzy rules were created considering all possible relevant scenarios. It is within the rule editor that fuzzified inputs (degrees of membership) are processed from the original crisp values obtained according to human-based conditional statements or fuzzy "If-then" rules.

As stated earlier, the logical "If-then" rule syntax was followed to formulate the conditional statements that encompass the fuzzy logic system. The first part of a rule (i.e., the "If" part) refers to the antecedent or the input within the rule. The input portion of a fuzzy rule is also the membership function of an element in a fuzzy set. The second part of the rule, called the "then" part, is known as the consequent or the system output associated to the fuzzy set. The combination of all inputs equals the possible number of rules. For the FST-based methodology, there are 36 fuzzy rules that have been defined.

The rule building process just described was created based on the academic literature reviewed, as well as discussions with subject matter experts. Experts were asked to assist in the creation and validation of every single fuzzy rule given their relevant knowledge combined with prior significant experience. Table 17 shows the input combination that results (or not) in the selection of an ISC according to the experts. For instance, the first rule below is to be read as follows:

*IF EIC is High AND Scope is Low AND Compliance is Comply AND Risk is Yes THEN ISC_Selected is Selected.*

Table 17. Rules to determine ISC Selection

| | EIC | Scope | Compliance | Risk | ISC_Selected |
|---|---|---|---|---|---|
| 1 | High | Low | Comply | Yes | Selected |
| 2 | High | Medium | Not Comply | Yes | Selected |
| 3 | High | Medium | Comply | Yes | Selected |
| 4 | High | High | Comply | No | Selected |
| 5 | High | High | Not Comply | Yes | Selected |
| 6 | High | High | Comply | Yes | Selected |
| 7 | Average | Low | Comply | Yes | Selected |
| 8 | Average | Medium | Comply | No | Selected |
| 9 | Average | Medium | Not Comply | Yes | Selected |
| 10 | Average | Medium | Comply | Yes | Selected |
| 11 | Average | High | Comply | No | Selected |
| 12 | Average | High | Not Comply | Yes | Selected |
| 13 | Average | High | Comply | Yes | Selected |
| 14 | Low | Low | Comply | No | Selected |
| 15 | Low | Low | Comply | Yes | Selected |
| 16 | Low | Medium | Comply | No | Selected |
| 17 | Low | Medium | Not Comply | Yes | Selected |
| 18 | Low | Medium | Comply | Yes | Selected |
| 19 | Low | High | Comply | No | Selected |
| 20 | Low | High | Not Comply | Yes | Selected |
| 21 | Low | High | Comply | Yes | Selected |
| 22 | High | Low | Not Comply | No | Not Selected |
| 23 | High | Low | Comply | No | Not Selected |
| 24 | High | Low | Not Comply | Yes | Not Selected |
| 25 | High | Medium | Not Comply | No | Not Selected |
| 26 | High | Medium | Comply | No | Not Selected |
| 27 | High | High | Not Comply | No | Not Selected |
| 28 | Average | Low | Not Comply | No | Not Selected |
| 29 | Average | Low | Comply | No | Not Selected |
| 30 | Average | Low | Not Comply | Yes | Not Selected |
| 31 | Average | Medium | Not Comply | No | Not Selected |
| 32 | Average | High | Not Comply | No | Not Selected |
| 33 | Low | Low | Not Comply | No | Not Selected |
| 34 | Low | Low | Not Comply | Yes | Not Selected |
| 35 | Low | Medium | Not Comply | No | Not Selected |
| 36 | Low | High | Not Comply | No | Not Selected |

### 4.1.4 Rule Viewer

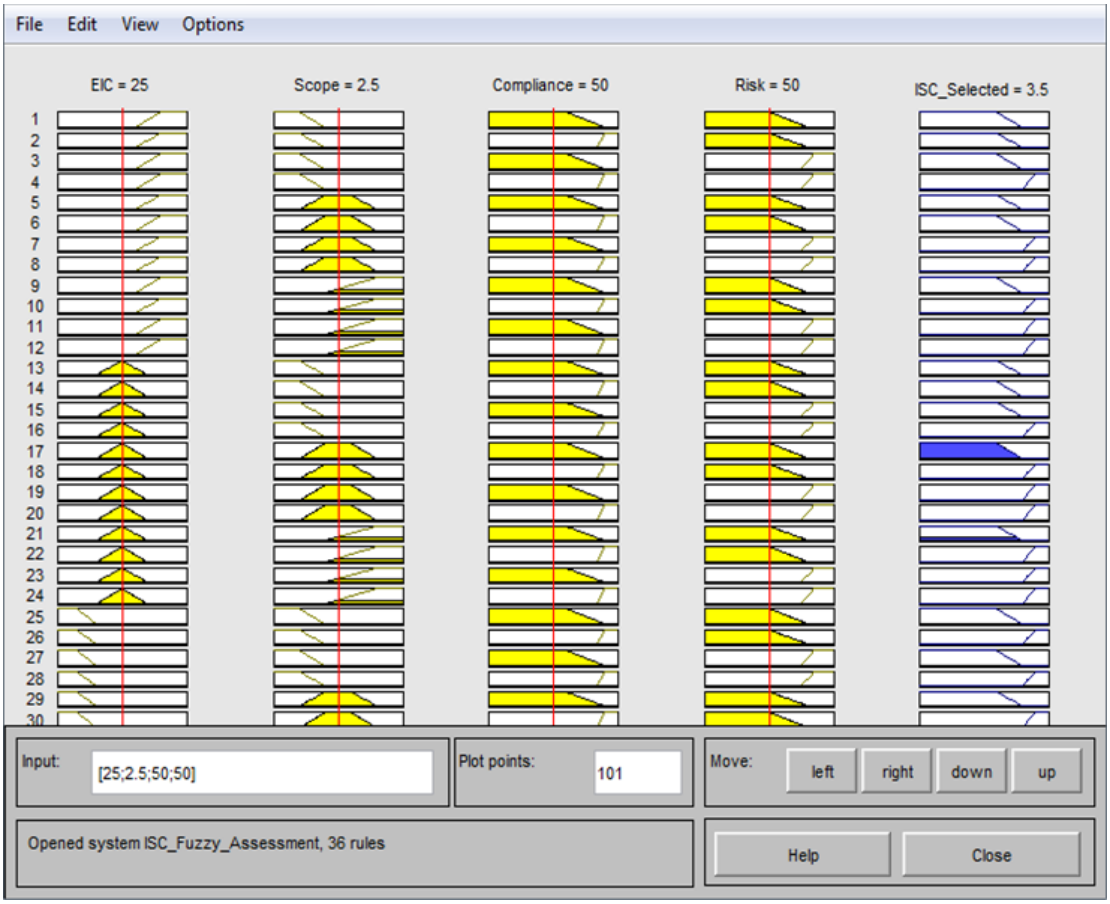



**Figure 17.** Rule Viewer

The rule viewer in Figure 17 displays the fuzzy rules that get triggered based on the input, and how the different membership functions affect the output. The output fuzzy set is obtained through finding one single crisp value that summarizes the fuzzy set. This is performed by taking the center of gravity and calculating the area of a combination of fuzzy sets. As stated in the Defuzzification section in Chapter three, the centroid approach (shown in equations 5 and 6) is employed to determine crisp values of the fuzzy output, as it is reliable and accurate when approximating the center of gravity (Genske & Heinrich, 2009). In the rule viewer, the number of rows is consistent with the number of

fuzzy rules defined (i.e., 36 in this case). Similarly, the columns displayed by the rule viewer refer to the defined membership functions for each input and output variable.

4.1.5 Surface Viewer

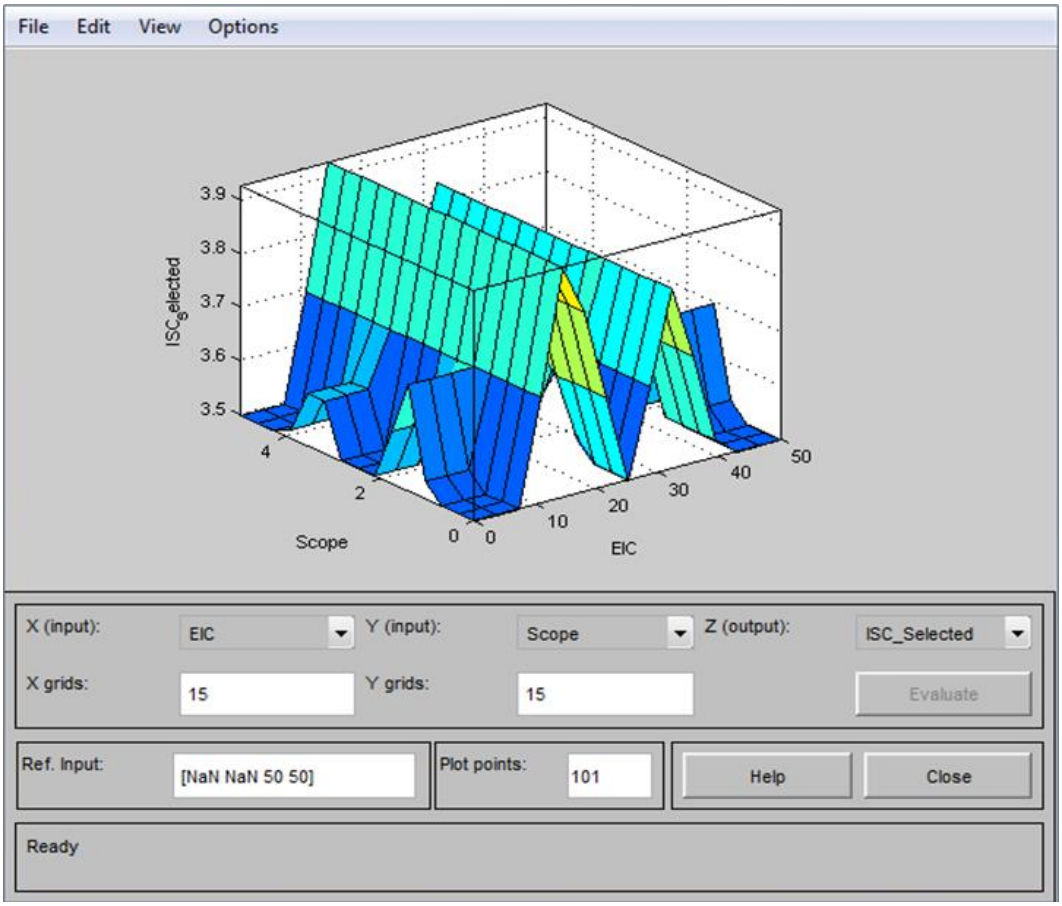



**Figure 18.** Surface Viewer

The purpose of the Surface Viewer is to generate and plot the entire output surface map for the system based on any two inputs and any one output in order to see a three-dimensional curve that represents the mapping from the inputs. Figure 18 illustrates the surface resulting from two input variables (Scope and EIC) in relation to the output variable (ISC_Selected). The Scope and EIC inputs were selected for demonstration purposes since, as stated, any two inputs can be selected. In this particular case, the

dependency of the output ISC_Selected in relation to the two inputs Scope and EIC is well represented by the output surface map.

Having developed the artifact, the next steps were to execute fuzzy logic over the actual data collected to prioritize ISC within the higher-ranked information security areas, as well as perform the required evaluations on the artifact.

**4.2 Results**

As stated earlier, the ISM ranked, in order of relevance, the 11 information security areas found in the ISO/IEC 27002. As instructed and for purposes of this dissertation, the ISM evaluated only the first three ranked information security areas. These were (in sequential order): Access Control, Compliance, and Human Resources Security. A significant advantage of the FST-methodology built herein, as stated before, is that it can accept and, thus, evaluate unlimited information security areas (not only three as included in this dissertation). For each ISC within the three information security areas identified as relevant, the ISM provided specific data related to literature-supported criteria (i.e., EIC, Scope, Compliance, and Risks).

The conclusions from fuzzy sets executed by the Toolbox were converted into real numbers, or single crisp values (i.e., Scores) through defuzzification. Defuzzification converts a fuzzy quantity to a precise quantity, represented by the logical union of two or more fuzzy membership functions defined on the universe of discourse of the output variable. In other words, defuzzification finds the one single crisp value that summarizes the fuzzy set. The defuzzification method used within this investigation, as discussed in Chapter three, was the center of gravity or centroid approach. The centroid approach

determines crisp values of the fuzzy output, and it is reliable and accurate when approximating the center of gravity.

Table 18 shows defuzzification, or the one single crisp value (Score) that summarizes the fuzzy set of logical inference results (or output fuzzy sets) for each ISC of the Access Control area after the FST-based methodology was executed.

Table 18. Access Control

| # | ISC Description | Score |
|---|---|---|
| 1 | An access control policy should be established, documented, and reviewed based on business and security requirements for access. | 9.18 |
| 2 | There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. | 3.81 |
| 3 | The allocation and use of privileges should be restricted and controlled. | 9.25 |
| 4 | The allocation of passwords should be controlled through a formal management process. | 8.59 |
| 5 | Management should review users' access rights at regular intervals using a formal process. | 9.14 |
| 6 | Users should be required to follow good security practices in the selection and use of passwords. | 9.14 |
| 7 | Users should ensure that unattended equipment has appropriate protection. | 3.50 |
| 8 | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. | 3.50 |
| 9 | Users should only be provided with access to the services that they have been specifically authorized to use. | 9.11 |
| 10 | Appropriate authentication methods should be used to control access by remote users. | 9.25 |
| 11 | Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. | 3.50 |
| 12 | Physical and logical access to diagnostic and configuration ports should be controlled. | 8.53 |
| 13 | Groups of information services, users, and systems should be segregated on networks. | 3.50 |
| 14 | For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications. | 3.81 |
| 15 | Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. | 3.81 |
| 16 | Access to operating systems should be controlled by a secure log-on procedure. | 9.25 |
| 17 | All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. | 9.14 |
| 18 | Systems for managing passwords should be interactive and should ensure quality passwords. | 8.67 |
| 19 | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | 9.14 |
| 20 | Inactive sessions should shut down after a defined period of inactivity. | 9.25 |
| 21 | Restrictions on connection times should be used to provide security for high-risk applications. | 8.77 |
| 22 | Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. | 9.07 |
| 23 | Sensitive systems should have a dedicated (isolated) computing environment. | 3.93 |
| 24 | A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities. | 3.53 |
| 25 | A policy, operational plans, and procedures should be developed and implemented for teleworking activities. | 3.78 |

Table 19 shows defuzzification for each ISC within the second relevant information security area, Compliance, after the FST-based methodology was executed.

Table 19. Compliance

| # | ISC Description | Score |
|---|---|---|
| 1 | All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. | 9.14 |
| 2 | Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. | 8.59 |
| 3 | Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. | 8.53 |
| 4 | Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. | 7.21 |
| 5 | Users should be deterred from using information processing facilities for unauthorized purposes. | 7.59 |
| 6 | Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. | 3.83 |
| 7 | Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. | 8.59 |
| 8 | Information systems should be regularly checked for compliance with security implementation standards. | 9.11 |
| 9 | Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. | 9.25 |
| 10 | Access to information systems audit tools should be protected to prevent any possible misuse or compromise. | 9.12 |

Defuzzification results for the last relevant information security area, Human Resources Security, are shown in Table 20, after the FST-based methodology was executed.

Table 20. Human Resources Security

| # | ISC Description | Score |
|---|---|---|
| 1 | Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy. | 9.05 |
| 2 | Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. | 3.54 |
| 3 | As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. | 3.53 |
| 4 | Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. | 5.33 |
| 5 | All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. | 8.59 |
| 6 | There should be a formal disciplinary process for employees who have committed a security breach. | 3.81 |
| 7 | Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. | 9.24 |
| 8 | All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement. | 3.50 |
| 9 | The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. | 9.10 |

Only ISC with scores of nine and higher are to be selected consistent with membership functions defined for the ISC_Selected fuzzy output variable in Table 16 and Figure 15. As a result, Tables 21, 22, and 23 show the ISC that should be selected, within each information security area, according to the FST-based methodology and membership functions defined.

Table 21. Access Control - ISC to be Selected

| # | ISC Description | Score |
|---|---|---|
| 1 | An access control policy should be established, documented, and reviewed based on business and security requirements for access. | 9.18 |
| 3 | The allocation and use of privileges should be restricted and controlled. | 9.25 |
| 5 | Management should review users' access rights at regular intervals using a formal process. | 9.14 |
| 6 | Users should be required to follow good security practices in the selection and use of passwords. | 9.14 |
| 9 | Users should only be provided with access to the services that they have been specifically authorized to use. | 9.11 |
| 10 | Appropriate authentication methods should be used to control access by remote users. | 9.25 |
| 16 | Access to operating systems should be controlled by a secure log-on procedure. | 9.25 |
| 17 | All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. | 9.14 |
| 19 | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | 9.14 |
| 20 | Inactive sessions should shut down after a defined period of inactivity. | 9.25 |
| 22 | Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. | 9.07 |

Table 22. Compliance - ISC to be Selected

| # | ISC Description | Score |
|---|---|---|
| 1 | All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. | 9.14 |
| 8 | Information systems should be regularly checked for compliance with security implementation standards. | 9.11 |
| 9 | Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. | 9.25 |
| 10 | Access to information systems audit tools should be protected to prevent any possible misuse or compromise. | 9.12 |

Table 23. Human Resources Security - ISC to be Selected

| # | ISC Description | Score |
|---|---|---|
| 1 | Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy. | 9.05 |
| 7 | Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. | 9.24 |
| 9 | The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. | 9.10 |

Tables 24, 25, and 26 display the ISC already implemented at the organization (before running the FST-based methodology) for each relevant information security area, as well as those identified for selection by the new FST artifact. Differences are noted between the two. This comparison is discussed and evaluated in detail in the next sub-

section to base the determination of whether information security in the organization is enhanced as a result of the new selection and evaluation of ISC (RQ2, H2).

Table 24. Access Control - Differences between ISC Already Implemented and ISC Selected per FST

| # | ISC Description | Already Implemented | Selected by FST | Difference Noted |
|---|---|---|---|---|
| 1 | An access control policy should be established, documented, and reviewed based on business and security requirements for access. | Yes | Yes | - |
| 2 | There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. | Yes | No | X |
| 3 | The allocation and use of privileges should be restricted and controlled. | No | Yes | X |
| 4 | The allocation of passwords should be controlled through a formal management process. | Yes | No | X |
| 5 | Management should review users' access rights at regular intervals using a formal process. | No | Yes | X |
| 6 | Users should be required to follow good security practices in the selection and use of passwords. | Yes | Yes | - |
| 7 | Users should ensure that unattended equipment has appropriate protection. | No | No | - |
| 8 | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. | Yes | No | X |
| 9 | Users should only be provided with access to the services that they have been specifically authorized to use. | Yes | Yes | - |
| 10 | Appropriate authentication methods should be used to control access by remote users. | Yes | Yes | - |
| 11 | Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. | No | No | - |
| 12 | Physical and logical access to diagnostic and configuration ports should be controlled. | No | No | - |
| 13 | Groups of information services, users, and information systems should be segregated on networks. | Yes | No | X |
| 14 | For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications. | Yes | No | X |
| 15 | Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. | No | No | - |
| 16 | Access to operating systems should be controlled by a secure log-on procedure. | No | Yes | X |
| 17 | All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. | Yes | Yes | - |

| # | ISC Description | Already Implemented | Selected by FST | Difference Noted |
|---|---|---|---|---|
| 18 | Systems for managing passwords should be interactive and should ensure quality passwords. | Yes | No | X |
| 19 | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | No | Yes | X |
| 20 | Inactive sessions should shut down after a defined period of inactivity. | No | Yes | X |
| 21 | Restrictions on connection times should be used to provide additional security for high-risk applications. | No | No | - |
| 22 | Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. | Yes | Yes | - |
| 23 | Sensitive systems should have a dedicated (isolated) computing environment. | No | No | - |
| 24 | A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities. | No | No | - |
| 25 | A policy, operational plans and procedures should be developed and implemented for teleworking activities. | No | No | - |

Table 25. Compliance - Differences between ISC Already Implemented and ISC Selected per FST

| # | ISC Description | Already Implemented | Selected by FST | Difference Noted |
|---|---|---|---|---|
| 1 | All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. | No | Yes | X |
| 2 | Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. | Yes | No | X |
| 3 | Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. | No | No | - |
| 4 | Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. | Yes | No | X |
| 5 | Users should be deterred from using information processing facilities for unauthorized purposes. | No | No | - |
| 6 | Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. | Yes | No | X |
| 7 | Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. | Yes | No | X |
| 8 | Information systems should be regularly checked for compliance with security implementation standards. | No | Yes | X |
| 9 | Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. | No | Yes | X |
| 10 | Access to information systems audit tools should be protected to prevent any possible misuse or compromise. | Yes | Yes | - |

Table 26. Human Resources Security - Differences between ISC Already Implemented and ISC Selected per FST

| # | ISC Description | Already Implemented | Selected by FST | Difference Noted |
|---|---|---|---|---|
| 1 | Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy. | Yes | Yes | - |
| 2 | Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. | No | No | - |
| 3 | As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. | Yes | No | X |
| 4 | Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. | Yes | No | X |
| 5 | All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. | Yes | No | X |
| 6 | There should be a formal disciplinary process for employees who have committed a security breach. | Yes | No | X |
| 7 | Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. | No | Yes | X |
| 8 | All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement. | Yes | No | X |
| 9 | The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. | Yes | Yes | - |

Next, evaluation of the artifact is performed. The evaluation is performed in two parts. First, the newly-created artifact is evaluated against other traditional ISC assessment methodologies to determine whether the weaknesses identified in existing and traditional ISC assessment methodologies (refer to Chapter two) have been addressed. Second, the new set of ISC generated from the artifact are assessed by a group of experts

against the organization's already-implemented ISC in order to determine whether such new set improves or not the current ISC selection process, as well as whether the overall information security in the organization is enhanced.

### 4.3 Evaluation of Artifact Against Traditional ISC assessment Methodologies

Following Hevner et al.'s (2004) DSR Guidelines and correspondent Process Steps from Vaishnavi and Kuechler's (2004) General Methodology of DSR, and consistent with Process Step 4: Evaluation, procedures were performed against existing and traditional ISC assessment methodologies. To evaluate the artifact and determine whether the ISC assessment methodology created using FST addressed the weaknesses identified in the literature for traditional assessment methodologies (RQ1), Hevner et al.'s (2004) suggest five design evaluation methods that include Observational (case studies, field studies); Analytical (static analysis, architectural analysis, optimization, dynamic analysis); Experimental (controlled experiments, simulations); Testing (functional, structural); and Descriptive (informed arguments, scenarios).

As stated earlier, evaluating the FST-based assessment methodology through performing comparisons and contrasts against existing ISC assessment methodologies found in the literature refer to the "Descriptive Design Evaluation Method" (Hevner et al., 2004). The Descriptive Design Evaluation Method prompts for comparisons between other existing ISC assessment methodologies, and assist in determining whether the artifact does enhance existing ISC assessment methodologies, satisfying the original requirements set in the research problem. The Descriptive Design Evaluation Method is also critical in evaluating and comparing the artifact's suitability and effectiveness against information from the knowledge base (i.e., existing ISC assessment

methodologies found in the literature) in order to build convincing arguments and/or scenarios and demonstrate the artifact's utility.

To properly evaluate the FST-based artifact developed herein, reference is made to Table 3, which lists the weaknesses identified in the academic literature on existing and traditional ISC assessment methodologies that preclude the effective assessment and, therefore, implementation of ISC in organizations over their information. The weaknesses referred to:

- involving high levels of subjectivity and ambiguity (van der Haar & von Solms, 2003);
- not adequately accounting for organizations' restrictions and constraints (van der Haar & von Solms, 2003);
- not preventing unnecessary ISC selections (Dhillon & Torkzadeh, 2006; Barnard & von Solms, 2000);
- not eliminating ad-hoc or random selections of ISC (Barnard & von Solms, 2000; Dhillon & Torkzadeh, 2006; Saint-Germain, 2005; Da Veiga & Eloff, 2007; Siougle & Zorkadis, 2002; Baskerville, 1993; Otero et al., 2010; van der Haar & von Solms, 2003; Ou Yang et al., 2011; Lv et al., 2011; Gerber & von Solms, 2008); and
- not considering all-inclusive, best practice scenarios when evaluating ISC (Ou Yang et al., 2011).

The weaknesses identified above not only affect the ISC selection process, but also impact the overall protection of the information's confidentiality, integrity, and availability (Saint-Germain, 2005). In other words, the lack of adequate information

security over valuable, sensitive, or critical financial information may allow for (1) fraud, manipulation, and/or misuse of data; (2) security-related deficiencies and findings; (3) bogus trades to inflate profits or hide losses; (4) false accounting journal entries; (5) computer security breaches; and (6) false transactions to evade regulators; among others. Refer to Figure 3.

Moreover, failure of paying adequate attention to address the weaknesses and/or inadequacies mentioned may allow opportunities for information security breaches which can negatively impact organizations, including their IT environments.

As illustrated in Table 3, as well as evidenced and discussed in Chapter four's Artifact Development, the FST-based ISC assessment methodology does address the weaknesses identified in traditional ISC evaluation processes specifically by:

(a) employing a less-subjective, ISC assessment approach. Even though the criteria input values (i.e., EIC, Scope, Compliance, and Risk) provided by the ISM reflects his opinion according to the organization's goals and objectives, those input values did not by themselves guide the ultimate decision for determining whether ISC should or should not be selected. In other words, the initial criteria input values provided by the ISM for each ISC, as specifically designed, were processed into the FST-based artifact, which contrary to traditional methods, involves a strict mathematical methodology, allowing for more precise and accurate ISC evaluation scores. As a result, bias and personal influences for determining ISC selection at the organization were significantly minimized by the FST-based artifact developed, as proposed.

(b) considering organizations' restrictions and constraints. The FST-based methodology developed herein allows any organization to adequately address their specific restrictions, constraints, goals, and/or objectives when determining which ISC to implement. In this particular case and in order to consider the organization's specific scenario and environment, the ISM provided input values for criteria considered relevant in the selection of ISC not only in the academic literature, but to the organization evaluated in this dissertation. The criteria evaluated herein referred to estimated implementation costs, scope, compliance with laws and regulations, and addressing the organization's risks, all four representing accepted evaluation criteria for ISC assessments based on the literature. By addressing specific restrictions and constraints (based on the above criteria), the FST artifact precisely evaluated and prioritized ISC for the organization.

(c) preventing or eliminating unnecessary and/or random selection of ISC. Contrary to many existing ISC methodologies, the FST-based assessment artifact created did not leave the identification and selection of ISC to the users. Precise evaluation scores per ISC resulted from strict mathematical calculations performed by FST. The use of the FST-based method developed prevented ISC to be selected (many times at random) by organization users which typically results in the potential inclusion of unnecessary ISC and/or exclusion of required ones. The FST-based methodology prevented unnecessary and random ISC selections, resulting in a crucial help to the organization to select only the most effective ISC

to mitigate information security risks, ultimately enhancing its overall information security.

(d) contemplating all-inclusive ISC scenarios. As evidenced, the FST-based methodology addressed this existing limitation by considering all available ISC for evaluation and potential inclusion. These ISC were obtained from the ISO/IEC 27002 standard best practice framework, which contains an all-inclusive list of ISC that can potentially be selected and implemented. Having identified relevant information security areas for the organization (Access Control, Compliance, and Human Resources Security), ISC within these areas were included for the ISM to evaluate by providing specific criteria information. The methodology then incorporated all ISC on its calculation and ultimate selection determination.

The FST-based ISC assessment methodology clearly enhanced current evaluation processes for ISC in the organization by (a) employing a less-subjective, accuracy-based method; (b) considering all possible organization's restrictions and constraints; (c) eliminating or preventing the random and unnecessary selection of ISC; and by (d) contemplating all-inclusive ISC scenarios. The FST-based assessment methodology adequately modeled imprecise parameters (i.e., criteria for determining ISC relevance), and addressed the weaknesses identified in existing methodologies, thereby addressing and supporting RQ1 and H1, respectively, both defined under section "Research Questions and Hypotheses".

Next, the new set of ISC generated from the artifact are assessed by a group of subject matter experts against the organization's already-implemented ISC in order to

determine to what extent does an ISC assessment methodology developed with FST enhance information security in the organization (RQ2).

### 4.4 Evaluation of Artifact's Results Against the Organization's Already Implemented ISC

A second and final evaluation consisted of determining to what extent the new ISC assessment methodology enhances information security in the organization (RQ2, H2). In order to respond to the above, subject matter experts were contacted and engaged to provide an evaluation focusing on:

- the ISC that were already implemented but identified by the FST artifact as *not* to be implemented; as well as

- ISC that were not already implemented, but identified by the FST artifact as *needed* to be implemented.

These differences noted are illustrated in Tables 24, 25, and 26.

The use of a panel of experts is very common and suitable for this type of evaluation and validation (Huang, Hung, Yen, Chang, & Jiang, 2011; Dhillon & Torkzadeh, 2006; Emory & Cooper, 1991). The criteria used for selecting the experts required a significant interest in the information security domain. There were three experts, each with 15-20 years of experience holding Management positions for global, also known as Big Four, accounting and audit firms. They also had significant auditing and consulting services on small-to-medium size type organizations within several industries, including the schools, universities, and non-profit industry, relevant for this dissertation. The experts' experience further included working for private industries, as well as for information systems and technology audit departments. All experts have performed work in Puerto

Rico as well as in the United States. The experts agreed to assist in the evaluation of the new set of ISC (via interview meetings and/or calls), resulting from the FST-based assessment methodology. Involvement of experts with the required knowledge, competency, and proficiency added significant value to this dissertation when interpreting and validating the results.

Before assessing the FST artifact, the experts were provided relevant information about the organization, as well as the expectations from their evaluation and validation tasks.

Table 24 shows the ISC for the Access Control information security area where differences were identified after running the FST assessment methodology. For instance, ISC 2, already implemented at the organization, should not be according to the FST methodology, while ISC 3 was not in place by the organization, but should now be. Tables 25 and 26 also show the ISC for the Compliance and Human Resource Security areas, respectively, where similar differences were identified after running the FST assessment methodology.

Experts were asked to compare the resulting set of ISC from the FST methodology against the ISC already implemented by the organization in order to determine whether the new set of ISC results in an enhancement to the information security of the organization. Specifically, the experts were provided copies of the results shown in Tables 24, 25, and 26, listing both, the ISC that were already implemented but identified by the FST artifact as *not* to be implemented; as well as the ISC that were not already implemented, but identified by the FST artifact as *needed* to be implemented (refer to "Difference Noted" column within Tables 24, 25, and 26). The experts were requested to

determine if additional information security risks within the three areas (Access Control, Compliance, and Human Resources Security) were addressed by the new set of ISC. Or, vice versa, whether information security risks were now not covered with the new set of ISC. The evaluation exercise prompted the experts to ultimately determine if the new set of ISC enhanced the information security of the organization.

Overall and based on numerous evaluation interviews and phone calls (captured and summarized in Appendix B), the experts were pleased with the new methodology and believed that the evaluation model could be useful for ISC assessment in practice, particularly, to:

- assist Management in planning its evaluation of ISC by referencing rigorous baseline manuals or best practice framework such as the ISO/IEC 27002 (2005);

- identify which ISC are of higher priority in relation to a specific, organizational-oriented assessment criteria; and

- communicate with other departments within the organization.

In a more detailed level (i.e., per information security area), the experts' main points as a result of their evaluation were as follows:

4.4.1 Access Control

- For this information security area, the experts concluded that the ISC that were identified as to be selected under the FST-based methodology, but had not been implemented (i.e., ISC 3, ISC 5, ISC 16, ISC 19, and ISC 20) addressed other relevant information security risks within the organization and, thus, added significant value and protection to the organization's financial information. Additional existing risks addressed by the new set of ISC are described below:

- Security parameters are not adequately configured, allowing for potential unauthorized user access to financially significant systems, applications, or databases.
- Privileges are granted to users which are not consistent with their job functions. The above allows unauthorized or incorrect modifications to financial data, resulting in segregation of duties conflicts, unprevented or undetected errors, incorrect financials, and/or management decisions based upon misleading information.
- Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information.
- Users with unauthorized accounts can change configuration settings or execute system administration activities to financial applications' parameters, giving rise to potential fraud, invalid data, failure to safeguard assets, or misled management.

On the contrary, the experts determined that those ISC that had been already implemented by the organization but were not identified as to be selected under the FST-based methodology (i.e., ISC 2, ISC 4, ISC 8, ISC 13, ISC 14, and ISC 18), did not necessarily pose a significant impact to the organization's financial information. In other words, the absence of such ISC within the organization did not represent a major concern to the financial information, as an adequate level of security was still in effect given the various other already-implemented ISC plus the new ISC resulting from the Fuzzy analysis (refer to Table 24), all of which mitigate access control risks and maintain proper levels of security.

4.4.2 Compliance

- For this information security area, the experts concluded that the ISC that were identified as to be selected under the FST-based methodology, but had not been implemented (i.e., ISC 1, ISC 8, and ISC 9) addressed relevant information security risks and, thus, added significant value and protection to the organization's financial information. Additional existing risks addressed by the new set of ISC are described below:

- Breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements take place over the design, operation, use, and management of information systems.

- Information systems are not in compliance with organizational security implementation policies, standards, and documented security controls.

- Operational systems and audit tools are not adequately safeguarded to prevent their misuse.

The experts determined that the ISC that had been already implemented but were not identified as to be selected under the FST-based methodology (i.e., ISC 2, ISC 4, ISC 6, and ISC 7) did not pose a significant impact to the organization's financial information. That is, the absence of such ISC within the organization did not represent a major effect to the financial information, as an adequate level of security would still be provided from the other implemented ISC.

4.4.3 Human Resources Security

- For this information security area, the experts concluded that the ISC that were identified as to be selected under the FST-based methodology (i.e., ISC 1, ISC 7, and ISC 9) were not sufficient in providing effective protection to financial information systems

or addressing relevant information security risks related to the Human Resources area. As seen, few ISC were selected by the FST-based methodology based on the actual data collected from the organization. In looking back at such data collected, noted that the EIC's provided to assess the selection and implementation of these Human Resources Security-related ISC were relatively high compared to the other two information security areas. Such increase in EIC's, as expected, impacted the ultimate selection of ISC within the Human Resources Security area. The experts suggested that ISC per the new methodology must be combined with the ISC originally implemented by the organization to maintain an adequate level of security within the organization financial assets. Refer to Appendix B, interview/call 25-32, 35-45, and 47. Given the above, the three experts determined that the new assessment methodology did not necessarily provide significant additional value to the Human Resources information security area, although it helped in strengthening the area.

- The experts determined that the combination of ISC already implemented at the organization plus the ones identified by the FST-based methodology (i.e., ISC 1, ISC 3, ISC 4, ISC 5, ISC 6, ISC 7, and ISC 8) provide a solid level of protection to the Human Resources Security area. For the organization, implementation of the above combined ISC helps address the following existing risks, thereby maintaining an enhanced level of information security.

- Employees, contractors, and third party users do not understand their responsibilities, and are not suitable for the roles they are considered for.

- The risk of theft, fraud or misuse of facilities is not reduced.

- Security responsibilities related to job descriptions and conditions of employment are not necessarily addressed prior to employment.
- All candidates for employment, contractors, and third party are not adequately screened, especially for sensitive jobs.
- Employees, contractors, and third party users are (1) not aware of information security threats and concerns, their responsibilities and/or liabilities; and (2) not equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
- An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities is not provided to all employees, contractors and third party users to minimize possible security risks.
- A formal disciplinary process for handling security breaches is not established.
- The exit process for employees, contractors, and third party is not performed effectively or in a timely or orderly manner. Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.
- Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information.

As evidenced, the ISC assessment methodology developed using FST had a positive impact on information security at the organization. The experts concurred that the implementation of the new set of ISC significantly enhanced the information security at the organization. Quotes and comments from the experts support the aforementioned

statement. Based on the interviews and calls conducted, the experts agreed that additional relevant information security risks within the three areas evaluated were addressed by the new set of ISC. Appendix B captures detailed information regarding these interviews and calls, including the date of the interview or call, relevant information security risk, expert number, whether it was an interview or a call, its duration, and determination, per expert, whether the relevant information security risk was addressed or not. After evaluation of such information, it was clear that RQ2 and H2, stated under section "Research Questions and Hypotheses" and prompting/posing whether an ISC assessment methodology that is developed using FST can enhance information security at the organization, were addressed and supported, respectively.

Consistent with the main goal of this dissertation, the assessment methodology developed and presented in this dissertation not only addressed the weaknesses identified in traditional methodologies, but also proved to improve information security at the organization. This turned out to be of crucial interest to the organization, as well as represented a valid contribution to the information security literature.

Equally significant, the methodology developed herein:

- can be easily implemented in a spreadsheet or software tool, and promote usage in practical scenarios where highly complex methodologies for ISC selection may become impractical;

- is easily extended to include additional evaluation criteria and features, and can evaluate ISC in various domains; and

- most importantly, addressed the gaps and weaknesses identified in the academic literature, as well as enhanced information security in organizations.

Overall, the FST-based assessment methodology proved to be a feasible technique for evaluating ISC in organizations.

**4.5 Summary**

This Chapter presented and discussed the results of this dissertation. Specifically, detailed explanations of the data collection process were provided, followed by descriptions of the development of the FST-based artifact and the Fuzzy Logic Toolbox of MATLAB editors and viewers used.

The artifact was built with the Fuzzy Logic Toolbox of MATLAB, which is used for solving problems with fuzzy logic. Such toolbox includes a collection of functions built on the MATLAB computing environment that provides technologies to create and modify fuzzy inference systems within the framework of MATLAB.

The toolbox comes with five editors and viewers defined to assist in building, editing, and viewing fuzzy inference systems, and links most of human reasoning and concept formation to fuzzy rules. In other words, the toolbox amplifies the power of human reasoning through providing a systematic framework for computing with fuzzy rules.

Findings and results of the FST-based artifact were next identified and explained, followed by evaluations of the artifact against other ISC assessment methodologies and second, against the organization's already implemented ISC. The second part of the evaluation was performed through interviews and meetings with three field and subject matter experts. The evaluation results provided responses to RQ 1 and RQ 2, and supported the proposed H1 and H2. Finally, the evaluation results supported the main contribution of this dissertation which was the development of an ISC assessment

methodology that could address existing weaknesses in traditional methodologies and, in turn, enhance information security in the organization.

The following chapter concludes this dissertation by providing the conclusions, implications, recommendations, and a final summary of the investigation work performed.

# Chapter 5

# Conclusions

## 5. Introduction

This Chapter states the conclusions based on the analysis performed and results achieved. The Chapter also delineates barriers, assumptions, limitations and delimitations of this dissertation. Further, this Chapter discusses the implications of the work on the field of study and its contributions to knowledge and professional practice. Recommendations for future research are presented next, followed by an overall summary of the work presented within this dissertation.

## 5.1 Conclusions

According to the DSR Guidelines in Hevner et al.'s (2004), and correspondent Process Steps from Vaishnavi and Kuechler's (2004) General Methodology of DSR, conclusion is the final process step where research results are documented. Results are also associated with clear and verifiable research contributions from the creation of the artifact and either support the objectives and direction of the investigation or simply evidence the opposite.

The goal of this dissertation was to develop an assessment methodology that (a) considers all-inclusive scenarios when evaluating ISC; (b) adequately accounts for organizations' restrictions and constraints; (c) significantly minimizes subjectivity and ambiguity (via providing precise evaluation values for ISC); and (d) prevents unnecessary and random ISC selections. The aforementioned can better assist

organizations when selecting ISC in order to mitigate information security risks, ultimately enhancing the overall information security. Refer to Table 2 and Figure 3.

Consistent with the above, the following RQ's were investigated:

RQ1: How does an ISC assessment methodology that is developed using FST address the weaknesses identified in the academic literature for traditional assessment methodologies?

RQ2: To what extent does an ISC assessment methodology developed with FST enhance information security in the organization?

Similarly, the following hypotheses (H) were proposed:

H1: An ISC assessment methodology that is constructed using FST contemplates all-inclusive ISC scenarios; employs a less-subjective, precision/accuracy-based method; prevents or eliminates the random and unnecessary selection of ISC; and considers organizations' restrictions and constraints when assessing ISC.

H2: An ISC assessment methodology developed with FST that addresses the weaknesses identified in traditional assessment methodologies enhances information security in the organization.

To address and test the research questions and hypotheses, data were collected via a questionnaire sent through email (see Appendix A) to an organization in Puerto Rico. The organization was a small-to-medium size organization within the industry of schools, universities, and not-for-profits. The questionnaire was emailed to the Information Security Manager (ISM). First, the ISM provided the ISC already in place at the organization that protect financial-related applications. The purpose of identifying the ISC already in place was to compare them with the ones generated by the newly-

developed methodology and evaluate, consistent with Hypothesis 2, whether the new set of ISC enhances information security in the organization. Second, the ISM ranked, in order of relevance, the 11 information security areas found in the ISO/IEC 27002 best practice framework and widely used in organizations to improve information and processes (Step 2). The ISM identified only the three most relevant information security areas based on the organization's goals and objectives. These were in specific order: Access Control, Compliance, and Human Resources Security. Finally, for each ISC within the three information security areas identified as relevant, and in order to start the assessment process, the ISM provided specific data related to a literature-supported criteria (i.e., EIC, Scope, Compliance, and Risks).

With the above data, the artifact was built using the Fuzzy Logic Toolbox of MATLAB ("toolbox"). The artifact consisted of four fuzzy input variables, each constituting a specific, literature-supported evaluation criteria (i.e., Estimated Implementation Cost (EIC), Scope, Compliance, and Risks), and one output variable named ISC_Selected. Next, membership functions were created for each particular input considering the literature reviewed as well as input from decision makers within the organization. Fuzzy "If-then" rules were then created considering all possible relevant scenarios. The rule building process described above was created based on the academic literature reviewed, as well as discussions with organization's decision makers. Table 17 shows the input combination that result in the selection of an ISC according to the experts.

With the artifact developed, the fuzzy logic was executed over the actual data collected, and results were produced. Only ISC with scores of nine and higher were selected consistent with membership functions defined.

The artifact was next evaluated; first, against traditional ISC assessment methodologies to determine whether the weaknesses identified in existing and traditional ISC assessment methodologies (refer to Chapter two) have been addressed. Second, the new set of ISC generated from the artifact were assessed by a group of experts against the organization's already-implemented ISC in order to determine whether such new set enhances the overall information security in the organization.

Based on the evaluations performed, the ISC assessment methodology developed using FST addressed the weaknesses identified in the academic literature for traditional assessment methodologies. In addition, the ISC assessment methodology had a positive effect over the information security at the organization, according to the experts. Because of the above, both, research questions RQ1 and RQ2, stated under section "Research Questions and Hypotheses" and prompting whether an ISC assessment methodology that is developed using FST address weaknesses in traditional ISC assessment methodologies, as well as enhance overall information security at the organization, were successfully addressed. The artifact developed herein, thus, represented a significant contribution to the organization and to the information security literature.

**5.2 Barriers and Issues**

The research problem within this dissertation was inherently difficult to solve because organizations are usually not willing to share data about their information security environments (Straub, 1986). That is, a barrier of this dissertation was the reticence of the

organization to have its environment evaluated for research purposes. Challenges were also encountered when attempting to select an organization that was truly interested in participating of this research. Given demanding schedules, organization's personnel felt reluctant in becoming part of this effort.

The creation of the FST-based ISC assessment solution within this dissertation was of adequate difficulty, meriting significant attention (i.e., dissertation-level work) as it attempted to correct weaknesses identified in traditional, highly practical ISC assessment methodologies. Further challenges were identified when determining whether the new methodology developed would indeed result in a more effective selection of ISC, thereby enhancing information security in organizations. A last barrier or issue, was the relative short period of time (i.e., three weeks) provided to the organization to complete the questionnaire, which may have not been appropriate and, therefore, posed potential concerns.

### 5.3 Assumptions

This dissertation assumed that an FST ISC assessment methodology can address the weaknesses identified in the literature. This dissertation also assumed that an improved ISC assessment methodology may have a positive impact on the information security of the organization.

In terms of data collection, this study assumed that responses from participants were true, reliable, and honest given that (a) the actual data collected was secured and available only for investigation and analysis purposes; (b) no personal information was attached nor disclosed to participants' responses in order to increase their confidence; (c) respondents were competent and directly affected by this research; and (d) the study's

research results were made available to interested participants, as recommended by Okoli and Pawlowski (2004).

Another assumption was that the target audience, key information security management personnel, is familiar with information security and, most importantly, has the required knowledge and relevant experience necessary to be part of this investigation. A last assumption within this dissertation was that the ISC assessment methodology built herein can adequately evaluate ISC in organizations within the schools, universities, and non-profit industry.

### 5.4 Implications for Research and Practice

The research presented in this dissertation developed an innovative approach for evaluating ISC in organizations in a more precise and accurate manner by addressing several weaknesses identified in the literature. Specifically, it presented a methodology that used FST to create a unified measurement that represented how well ISC met specific organization criteria. Through the evaluation performed in this dissertation for a single organization, the methodology was proven successful in providing a way for measuring the quality of ISC.

In terms of research implications, the ISC assessment methodology evidenced a more accurate and precise evaluation and prioritization of ISC, which clearly advanced the current information security literature. For practical purposes, the methodology is expected to assist organizations' management in: 1) correcting weaknesses and inadequacies in existing ISC assessment methodologies, thereby, providing for a more effective selection of ISC; 2) granting efficient investment of resources; and 3) enhancing the overall information security in organizations.

The main contribution of this research to the information security literature is the development of a FST-based assessment methodology that provides for a thorough evaluation of ISC in organizations. The methodology created addresses the weaknesses or limitations identified in existing ISC assessment methodologies, resulting in an enhanced information security in organizations.

An ISC assessment methodology based on FST provides benefits and advantages over traditional methods, including a strict mathematical methodology that can precisely and rigorously examine vague conceptual phenomena (Zimmermann, 2001). Additionally, FST has been used as a modeling, problem solving, and data mining tool, and has proven superior to existing methods, as well as attractive to enhance classical approaches.

Klir and Yuan (1995) also point the significance of FST when handling uncertainty. FST helps in understanding the phenomenon of reality by performing adequate predictions or retrodictions; learning about controlling the phenomenon; and utilizing such capabilities for various other ends. Furthermore, a FST-based framework leads to more detailed and thorough assessments, while appropriately modeling human decisions related to ISC evaluation, which are imprecise in nature (Petrovic-Lazarevic, 2001).

A suitable FST-based ISC assessment methodology accounts for imprecise parameters and criteria when calculating the relevance of ISC. Such evaluation is also focused on how well ISC address organization goals, objectives, restrictions, risks, laws, and regulations. Results from this research supported that a FST-based methodology assisted the organization in evaluating and, thus, determining and selecting only the most effective ISC. The methodology presented also laid down the foundation for the

development of a fuzzy expert system as a solution to the ISC existing evaluation and ranking problem.

Other contributions from the methodology created in this dissertation include that it:

- is relatively simple, can be implemented in a spreadsheet or software tool, and promote usage in practical scenarios where highly complex methodologies for ISC selection are impractical.
- fuses multiple evaluation criteria to provide a holistic view of the overall quality of ISC.
- is easily extended to include additional evaluation criteria factor not considered within this dissertation (this is possibly on of the most meaningful contribution from this dissertation).
- provides a mechanism to evaluate the quality of ISC in various domains.

Overall, the methodology presented in this dissertation proved to be a feasible technique for evaluating ISC in organizations.

**5.5 Limitations and Recommendations for Future Research**

A key advantage of using a FST-based decision support model for ISC evaluation is that it provides a natural, effective way of handling problems in which the source of imprecision is the absence of sharply defined criteria. Nevertheless, the solution requires the specification of membership functions of fuzzy sets, definitions of linguistic variables, and fuzzy operators in order to model the attitudes and assumptions of organizations regarding the relevance of ISC. In other words, fuzzy sets must be specified with regard to the objective function, constraints established, as well as terms and membership functions of the linguistic variables. Further empirical work would contribute to identify the aforementioned attitudes and assumptions of decision makers

within organizations. Despite the limitation stated above, it was argued throughout this dissertation that a FST-based perspective of evaluating ISC is a valuable tool for organizations when dealing with uncertainty and imprecision.

There were other limitations associated with this dissertation study. First, due to convenience and availability, this dissertation involved a single, Puerto Rico-based, small-to-medium size type organization within the schools, universities, and non-profit industry. Therefore, findings can be generalized to similar size type and industry organizations located in Puerto Rico. Further similar studies may be needed at organizations outside of Puerto Rico, or from different sizes and industry types within Puerto Rico in order to generalize the findings of this dissertation in a broader scope.

Second, the questionnaire used in this dissertation was completed by the organization within a three week timeframe. A longitudinal study may add significant value as organization goals, objectives, and laws and regulations, among others, shift over time and, thus, the need to select and implement different ISC. Organizations must periodically reassess their ISC implementation and adjust their selection criteria consistent with new goals, objectives, laws, and regulations.

Third, Tichy (1998) as well as Zelkowitz and Wallace (1998), stressed that implementing a DSR's developed artifact in a single organization (as is the case in this dissertation) represents a challenge, as results may not be generalizable to other organizations or environments. Implementation of the DSR research method further 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. DSR results can be outrun by technology before they even show up in the research literature (Hevner et al., 2004).

Regarding future work, the following opportunities extend the research conducted within this dissertation:

- investigate whether it is reasonable to develop fuzzy rules and baselines of membership functions for ISC in particular environments.
- interview experts from organizations within similar industries in order to identify fuzzy sets for ISC assessments that can potentially be utilized as guidelines/standards across organizations within similar industries.
- add criteria factors to evaluate ISC other than the ones included in this dissertation. Refinement or the incorporation of additional assessment factors, specifically targeting organization's restrictions, goals, objectives, regulations, etc., can certainly improve the current investigation.
- examine results from this dissertation and compare them to other assessment results from other similar organizations.

Another potential direction for future research considers utilizing a hybrid approach, using FST and traditional methodologies, to assess ISC. As evidenced in this dissertation, when assessing ISC within the Human Resources Security area, the FST-based methodology did not output a better selection of ISC to protect financial information systems or address relevant information security risks. Applying a hybrid approach to assess ISC could not only extend the work performed in this dissertation, but can also strengthen current ISC evaluation and selection processes in organizations.

Future research can develop more interactive and more user friendly application programs for ISC evaluation. Finally, more case studies should be conducted within the industry evaluated in this study (i.e., schools, universities, and not-for-profits) and use those results to construct the related norm database of evaluation model for the establishment of industrial best practice examples.

**5.6 Delimitations**

A critical part of the scope of this dissertation is related to the information systems that were involved. That is, the information systems and applications where ISC were evaluated for comprised only financial-related systems and applications. All other systems and/or applications within the selected organization (e.g., operational-purpose applications, databases, operating systems, networks, etc.) were not in scope for purposes of this dissertation, although the methodology is flexible enough to also consider other systems and applications.

Additionally, the target audience comprised only key information security personnel (i.e., Information Security Manager). Due to their knowledge and experience, the target audience reflects an accurate representation of the population, allowing for results to be generalizable and, thus, consistently applied to other small-to-medium size type organizations, as considered herein (Salkind, 2009). Requests for participation were made to small-to-medium size type organizations within a specific industry (i.e., schools, universities, and non-profit). The targeted organization was located in the state of Puerto Rico and was contacted based on convenience and availability.

Another delimitation used to constrain the scope of this dissertation referred to the specific membership functions of fuzzy sets, linguistic variables, and fuzzy operators that

were used to model the particular attitudes and assumptions of decision makers when assessing ISC. That is, the membership functions used to represent fuzzy numbers within this dissertation were restricted to some of the most common ones (i.e., triangular and trapezoidal), which are preferred due to their combination of solid theoretical basis and simplicity (Pedrycz, 1994). The linguistic variables or linguistic terms in this study were limited to four factors: (1) Estimated Implementation Cost, (2) Scope, (3) Compliance, and (4) Risks, which represent an accepted evaluation criteria for ISC assessments based on the literature. Lastly, fuzzy operators were limited to 'AND' and 'OR' to assist fuzzy rules when implying fuzzy relationships between antecedents and consequences. The fuzzy operator 'AND' evaluated the intersection or conjunction of the rule antecedents, while the fuzzy operator 'OR' assessed the union or disjunction of the rule antecedents. The 'NOT' operator known as the fuzzy complement was not used in this dissertation. Regarding the limitation stated earlier involving DSR's results being potentially upset by technology before they are implemented in organizations, or before they appear in the research literature, Hevner et al. (2004) argue that the implementation of DSR results from well-designed IT artifacts still impact organizations significantly, as they "enable organizations to address important information-related tasks" (p. 98). Rapid advances in technology can potentially overturn research results before their implementation, or publishing in the literature, resulting in a common risk to all research methods. However, DSR mitigated the aforementioned by engaging active technology in the creation of its artifacts and by providing effective results and solutions to current organizational problems.

## 5.7 Summary

Adequate evaluation of ISC is crucial to organizations in maintaining a sound information security as well as in protecting their information assets. Nevertheless, the literature points out several issues, gaps, weaknesses, and/or inadequacies within traditional ISC assessment methodologies that prevent an effective assessment of ISC in organizations. The goal or research problem addressed by this dissertation was the need for development of an ISC assessment tool that could address weaknesses identified in traditional ISC assessment methodologies, and potentially enhance ISC evaluations as well as overall information security in the organization. Based on a comprehensive review of relevant literature (see Table 2), there are evident weaknesses in existing assessment methodologies for ISC in organizations that can preclude an effective selection. Risks resulting from those weaknesses include inaccurate or incomplete processing of data; unauthorized access to data that might destroy or manipulate data (or report logic) in a fraudulently or unintentionally way; as well as the potential loss of data or inability to access data as required (PCAOB).

Consistent with the above, the purpose of developing a FST-based ISC assessment methodology was to enhance current evaluation processes by addressing weaknesses via employing a less-subjective, precision/accuracy-based method; eliminating or preventing the random and unnecessary selection of ISC; considering organizations' restrictions and constraints; and improving the overall information security in organizations. Similarly, it was argued that a FST-based assessment methodology allows for the modeling of imprecise parameters, resulting in a more accurate assessment, which was crucial to

determine the best ISC. Surprisingly, such a methodology had not been proposed within the information security literature based on the thorough review performed.

Research questions and hypotheses were raised based on the information, arguments, and claims presented (refer to Figure 2), and related to whether an ISC assessment methodology developed using FST addressed the weaknesses identified in the literature, as well as whether it ultimately enhanced information security in organizations.

This dissertation followed the DSR method, which is fundamentally a problem-solving paradigm (Simon, 1996). DSR creates and evaluates IT artifacts intended to solve identified organizational problems. Hevner et al. (2004) list seven guidelines that are crucial in understanding the requirements for effective DSR. Similar to Hevner et al.'s (2004) guidelines, Vaishnavi and Kuechler (2004) also developed a general method underlying DSR. Their method included only five process steps, which represent a summarized version of Hevner et al.'s (2004) seven DSR guidelines (see Table 4). Vaishnavi and Kuechler (2004) further identified expected outputs for their five DSR process steps. The Vaishnavi and Kuechler's (2004) five-process-steps General Methodology of DSR was followed in this dissertation.

To create the artifact (i.e., FST-based ISC assessment methodology), specific data from the organization were collected via questionnaire. The questionnaire was provided to the Information Security Manager from a small-to-medium size organization in Puerto Rico within the schools, universities, and not-for-profit industry.

Upon receipt of the questionnaire, the ISM identified the ISC already in place at the organization that protect financial-related applications. All other applications and/or information systems within the organization (e.g., applications, databases, operating

systems, networks in place for operational/non-financial purposes, etc.) were out of scope for purposes of this dissertation. The purpose of identifying the ISC already in place was to compare them with the ones generated by the newly-developed methodology and evaluate, consistent with Hypothesis 2, whether the new set of ISC enhanced information security in the organization. The ISC were selected from an all-inclusive list of ISC from the ISO/IEC 27002 best practice framework.

Following identification of the ISC currently implemented, the ISM ranked, in order of relevance, the 11 information security areas found in the ISO/IEC 27002 best practice framework. As instructed, the ISM identified only the three most relevant information security areas based on the organization's goals and objectives. These were in sequential order: Access Control, Compliance, and Human Resources Security.

For each ISC within the three information security areas identified as relevant, and in order to start the assessment process, the ISM provided specific data related to literature-supported criteria (i.e., EIC, Scope, Compliance, and Risks).

With the specific information collected from the organization, the artifact was built using the Fuzzy Logic Toolbox of MATLAB ("toolbox"). The toolbox is an instrument for solving problems with fuzzy logic.

For purposes of the FST-based artifact being created, there were four fuzzy input variables defined (also known as linguistic terms), each constituting specific, literature-supported evaluation criteria (i.e., Estimated Implementation Cost (EIC), Scope, Compliance, and Risks). Refer to Figure 9. Membership functions and relevant rules were then created for each particular input considering the literature reviewed, and decision makers within the organization. Experts were asked to assist in the creation and

validation of every single fuzzy rule used for purposes of this dissertation given their significant experience combined with their prior knowledge. Table 17 shows the input combination that result in the selection of an ISC according to the experts. Once the artifact was developed, the next steps were to execute fuzzy logic over the actual data collected to prioritize ISC within the higher-ranked information security areas, as well as evaluate the artifact.

As stated earlier, the ISM provided specific data related to literature-supported criteria (i.e., EIC, Scope, Compliance, and Risks). The conclusions from fuzzy sets executed by the Toolbox were converted into real numbers, or a single crisp values (i.e., Score) through defuzzification. Tables 18 through 20 showed defuzzification for the Access Control, Compliance, and Human Resources Security areas after the FST-based methodology was executed. ISC with scores of nine and higher were selected consistent with membership functions defined for the ISC_Selected fuzzy output in Table 16 and Figure 15.

With the generated scores, evaluation of the artifact was performed in two steps:

(1) by evaluating against other ISC assessment methodologies to determine whether the weaknesses identified in existing and traditional ISC assessment methodologies have been addressed; and

(2) the new set of ISC generated from the artifact are assessed by a group of experts against the organization's already-implemented ISC in order to determine whether such new set improves or not the current ISC selection process, as well as whether the overall information security in the organization is enhanced.

Per evaluation results, the FST-based ISC assessment methodology addressed the weaknesses in traditional methodologies, resulting in a more accurate assessment and selection of ISC, thereby addressing and supporting RQ1 and H1, respectively.

Experts then assisted in determining whether the new set of ISC enhanced information security at the organization. Overall, the experts concurred that the implementation of the new artifact significantly enhanced the overall information security at the organization. As a result, RQ2 and H2, stated under section "Research Questions and Hypotheses" and prompting whether an ISC assessment methodology that is developed using FST does enhance information security at the organization, were addressed and supported.

The assessment methodology developed in this dissertation precisely evaluated and prioritized ISC which, without a doubt, turned out to be of crucial interest to the organization. Such methodology also represented a valid contribution to the information security literature. Particularly, the methodology addressed gaps and weaknesses identified in the academic literature, as well as resulted in a more accurate selection of ISC which, in turn, enhanced information security in the organization.

Research studies continue to support the harmful effects of unsuccessful and/or weak information security platforms which results in opportunities for fraud, manipulation of information, and computer breaches, among others. Through a review of the literature, various key weaknesses were identified when assessing ISC in organizations. The methodology developed herein proved successful in assisting an organization selecting the most appropriate ISC for implementation, while also maintaining a well-designed and controlled information system security environment.

# Appendix A. Survey Questionnaire

Survey Questionnaire

An Information Security Control
Assessment Methodology for Organizations
Fort Lauderdale-Davie, Florida 33314

October 14, 2013

Dear Respondent:

I am a doctoral student conducting a survey to determine whether a newly-developed methodology corrects weaknesses identified in existing and traditional information security controls (ISC) assessment methodologies, and will result in a more effective selection of ISC, ultimately enhancing the overall information security in the organization. Please note that your feedback is valuable in addressing the aforementioned investigation.

In order to ensure the utmost privacy, the completed survey will not be made available to anyone other than the research team. Also, note that completing and submitting the survey indicate your voluntary participation in the study.

Kindly respond on or before November 1, 2013. I appreciate your time and assistance in furthering this research endeavor.

Cordially,

*/s/ Angel R. Otero*
Angel R. Otero
Doctoral Student
Graduate School of Computer and Information Sciences
Nova Southeastern University
Fort Lauderdale, Florida 33314
ao269@nova.edu

**STEP 1 - CURRENT INFORMATION SECURITY CONTROLS (ISC) AT THE ORGANIZATION**

**INSTRUCTIONS:** Below there is an all-inclusive list of information security controls (ISC) based on the International Organization for Standardization (ISO) / International Electro technical Commission (IEC) 27002:2005, considered a best practice framework.

**Please mark with an "X" the ISC already in place (implemented) at your Organization.**

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | | **Security Policy** |
| | 1 | An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. |
| | 2 | The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. |
| | | **Organization of Information Security** |
| | 1 | Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. |
| | 2 | Information security activities should be coordinated by representatives from different parts of the organization with relevant roles and job functions. |
| | 3 | All information security responsibilities should be clearly defined. |
| | 4 | A management authorization process for new information processing facilities should be defined and implemented. |
| | 5 | Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed. |
| | 6 | Appropriate contacts with relevant authorities should be maintained. |
| | 7 | Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. |
| | 8 | The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur. |
| | 9 | The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. |
| | 10 | All identified security requirements should be addressed before giving customers access to the organization's information or assets. |
| | 11 | Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or |

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | | adding products or services to information processing facilities should cover all relevant security requirements. |
| | | **Asset Management** |
| | 1 | All assets should be clearly identified and an inventory of all important assets drawn up and maintained. |
| | 2 | All information and assets associated with information processing facilities should be owned by a designated part of the organization. |
| | 3 | Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented. |
| | 4 | Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. |
| | 5 | An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. |
| | | **Human Resources Security** |
| | 1 | Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy. |
| | 2 | Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. |
| | 3 | As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. |
| | 4 | Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. |
| | 5 | All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. |
| | 6 | There should be a formal disciplinary process for employees who have committed a security breach. |
| | 7 | Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. |
| | 8 | All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement. |
| | 9 | The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon |

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | | change. |
| | | **Physical And Environmental Security** |
| | 1 | Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities. |
| | 2 | Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. |
| | 3 | Physical security for offices, rooms, and facilities should be designed and applied. |
| | 4 | Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. |
| | 5 | Physical protection and guidelines for working in secure areas should be designed and applied. |
| | 6 | Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. |
| | 7 | Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |
| | 8 | Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. |
| | 9 | Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. |
| | 10 | Equipment should be correctly maintained to ensure its continued availability and integrity. |
| | 11 | Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises. |
| | 12 | All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. |
| | 13 | Equipment, information or software should not be taken off-site without prior authorization. |
| | | **Communications and Operations Management** |
| | 1 | Operating procedures should be documented, maintained, and made available to all users who need them. |
| | 2 | Changes to information processing facilities and systems should be controlled. |
| | 3 | Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. |
| | 4 | Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system. |
| | 5 | It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, |

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | | operated, and maintained by the third party. |
| | 6 | The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly. |
| | 7 | Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks. |
| | 8 | The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. |
| | 9 | Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. |
| | 10 | Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. |
| | 11 | Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing. |
| | 12 | Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy. |
| | 13 | Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. |
| | 14 | Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced. |
| | 15 | There should be procedures in place for the management of removable media. |
| | 16 | Media should be disposed of securely and safely when no longer required, using formal procedures. |
| | 17 | Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse. |
| | 18 | System documentation should be protected against unauthorized access. |
| | 19 | Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. |
| | 20 | Agreements should be established for the exchange of information and software between the organization and external parties. |
| | 21 | Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization’s physical boundaries. |
| | 22 | Information involved in electronic messaging should be appropriately protected. |
| | 23 | Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems. |
| | 24 | Information involved in electronic commerce passing over public networks should |

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | | be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. |
| | 25 | Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. |
| | 26 | The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification. |
| | 27 | Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. |
| | 28 | Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. |
| | 29 | Logging facilities and log information should be protected against tampering and unauthorized access. |
| | 30 | System administrator and system operator activities should be logged. |
| | 31 | Faults should be logged, analyzed, and appropriate action taken. |
| | 32 | The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source. |
| | | **Access Control** |
| | 1 | An access control policy should be established, documented, and reviewed based on business and security requirements for access. |
| | 2 | There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. |
| | 3 | The allocation and use of privileges should be restricted and controlled. |
| | 4 | The allocation of passwords should be controlled through a formal management process. |
| | 5 | Management should review users' access rights at regular intervals using a formal process. |
| | 6 | Users should be required to follow good security practices in the selection and use of passwords. |
| | 7 | Users should ensure that unattended equipment has appropriate protection. |
| | 8 | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. |
| | 9 | Users should only be provided with access to the services that they have been specifically authorized to use. |
| | 10 | Appropriate authentication methods should be used to control access by remote users. |
| | 11 | Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. |
| | 12 | Physical and logical access to diagnostic and configuration ports should be controlled. |
| | 13 | Groups of information services, users, and information systems should be segregated on networks. |

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | 14 | For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications. |
| | 15 | Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. |
| | 16 | Access to operating systems should be controlled by a secure log-on procedure. |
| | 17 | All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. |
| | 18 | Systems for managing passwords should be interactive and should ensure quality passwords. |
| | 19 | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. |
| | 20 | Inactive sessions should shut down after a defined period of inactivity. |
| | 21 | Restrictions on connection times should be used to provide additional security for high-risk applications. |
| | 22 | Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. |
| | 23 | Sensitive systems should have a dedicated (isolated) computing environment. |
| | 24 | A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities. |
| | 25 | A policy, operational plans and procedures should be developed and implemented for teleworking activities. |
| | | **Information Systems Acquisition, Development And Maintenance** |
| | 1 | Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls. |
| | 2 | Data input to applications should be validated to ensure that this data is correct and appropriate. |
| | 3 | Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. |
| | 4 | Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented. |
| | 5 | Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. |
| | 6 | A policy on the use of cryptographic controls for protection of information should be developed and implemented. |
| | 7 | Key management should be in place to support the organization's use of |

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | | cryptographic techniques. |
| | 8 | There should be procedures in place to control the installation of software on operational systems. |
| | 9 | Test data should be selected carefully, and protected and controlled. |
| | 10 | Access to program source code should be restricted. |
| | 11 | The implementation of changes should be controlled by the use of formal change control procedures. |
| | 12 | When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. |
| | 13 | Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled. |
| | 14 | Opportunities for information leakage should be prevented. |
| | 15 | Outsourced software development should be supervised and monitored by the organization. |
| | 16 | Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. |
| | | **Information Security Incident Management** |
| | 1 | Information security events should be reported through appropriate management channels as quickly as possible. |
| | 2 | All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services. |
| | 3 | Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. |
| | 4 | There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. |
| | 5 | Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). |
| | | **Business Continuity Management** |
| | 1 | A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity. |
| | 2 | Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. |
| | 3 | Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. |

| Select with an "X" | | Information Security Area / ISC Description |
|---|---|---|
| | 4 | A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. |
| | 5 | Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective. |
| | | **Compliance** |
| | 1 | All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. |
| | 2 | Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. |
| | 3 | Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. |
| | 4 | Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. |
| | 5 | Users should be deterred from using information processing facilities for unauthorized purposes. |
| | 6 | Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. |
| | 7 | Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. |
| | 8 | Information systems should be regularly checked for compliance with security implementation standards. |
| | 9 | Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. |
| | 10 | Access to information systems audit tools should be protected to prevent any possible misuse or compromise. |

**STEP 2 - RANKING ISO/IEC 27002:2005 INFORMATION SECURITY AREAS**

**INSTRUCTIONS:** Below there is a list of the ISO/IEC 27002:2005 Information Security Areas. **Please rank these areas in order of relevance in relation to your organization from 1 - 11** ("1" representing the most important). For example, Access Management may be "1", Compliance "2", Business Continuity Management "3", and so forth.

| Rank in order of relevance from 1 - 11. | ISO/IEC 27002:2005 Information Security Area |
|---|---|
| | Security Policy |
| | Organization of Information Security |
| | Asset Management |
| | Human Resources Security |
| | Physical And Environmental Security |
| | Communications and Operations Management |
| | Access Control |
| | Information Systems Acquisition, Development and Maintenance |
| | Information Security Incident Management |
| | Business Continuity Management |
| | Compliance |

## STEP 3 - EVALUATION OF LITERATURE-SUPPORTED CRITERIA

Please assess the four-criteria below for each ISC listed. **Note:** As instructed and for purposes of this investigation, please perform the evaluation below for only the first three ranked information security areas identified in STEP 2.

### Security Policy

| | ISC Description - Security Policy | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. | | | | |
| 2 | The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing*

resource personnel as part of their daily responsibilities.

## Organization of Information Security

| | ISC Description - Organization of Information Security | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. | | | | |
| 2 | Information security activities should be coordinated by representatives from different parts of the organization with relevant roles and job functions. | | | | |
| 3 | Allocation of information security responsibilities: All information security responsibilities should be clearly defined. | | | | |
| 4 | A management authorization process for new information processing facilities should be defined and implemented. | | | | |
| 5 | Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed. | | | | |
| 6 | Appropriate contacts with relevant authorities should be maintained. | | | | |
| 7 | Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. | | | | |
| 8 | The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be | | | | |

| | ISC Description - Organization of Information Security | Estimated Implementation Cost (in thousands) ** | Scope - Number of systems/applications protected by ISC. [1, More than 1] | Extent to which the ISC Complies with required, external laws and regulations [0 - 100%] | Extent to which the ISC addresses information security risks [0 - 100%] |
|---|---|---|---|---|---|
| | reviewed independently at planned intervals, or when significant changes to the security implementation occur. | | | | |
| 9 | The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. | | | | |
| 10 | All identified security requirements should be addressed before giving customers access to the organization's information or assets. | | | | |
| 11 | Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Asset Management

| | ISC Description - Asset Management | Estimated Implementation Cost (in thousands) ** | Scope - Number of systems/applications protected by ISC. [1, More than 1] | Extent to which the ISC Complies with required, external laws and regulations [0 - 100%] | Extent to which the ISC addresses information security risks [0 - 100%] |
|---|---|---|---|---|---|
| 1 | All assets should be clearly identified and an inventory of all important assets drawn up and maintained. | | | | |

| | ISC Description - Asset Management | Estimated Implementation Cost (in thousands) ** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 2 | All information and assets associated with information processing facilities should be owned by a designated part of the organization. | | | | |
| 3 | Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented. | | | | |
| 4 | Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. | | | | |
| 5 | An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Human Resources Security

| | ISC Description - Human Resources Security | Estimated Implementation Cost (in thousands) ** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy. | | | | |

| | **ISC Description - Human Resources Security** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 2 | Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. | | | | |
| 3 | As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. | | | | |
| 4 | Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. | | | | |
| 5 | All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. | | | | |
| 6 | There should be a formal disciplinary process for employees who have committed a security breach. | | | | |
| 7 | Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. | | | | |
| 8 | All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their | | | | |

| | ISC Description - Human Resources Security | Estimated Implementation Cost (in thousands) ** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| | employment, contract or agreement. | | | | |
| 9 | The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Physical and Environmental Security

| | ISC Description - Physical And Environmental Security | Estimated Implementation Cost (in thousands) ** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities. | | | | |
| 2 | Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. | | | | |
| 3 | Physical security for offices, rooms, and facilities should be designed and applied. | | | | |
| 4 | Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms | | | | |

| | **ISC Description - Physical And Environmental Security** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| | of natural or man-made disaster should be designed and applied. | | | | |
| 5 | Physical protection and guidelines for working in secure areas should be designed and applied. | | | | |
| 6 | Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. | | | | |
| 7 | Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. | | | | |
| 8 | Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. | | | | |
| 9 | Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. | | | | |
| 10 | Equipment should be correctly maintained to ensure its continued availability and integrity. | | | | |
| 11 | Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises. | | | | |
| 12 | All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. | | | | |

| | ISC Description - Physical And Environmental Security | Estimated Implementation Cost (in thousands) ** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 13 | Equipment, information or software should not be taken off-site without prior authorization. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Communications and Operations Management

| | ISC Description - Communications and Operations Management | Estimated Implementation Cost (in thousands) ** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | Operating procedures should be documented, maintained, and made available to all users who need them. | | | | |
| 2 | Changes to information processing facilities and systems should be controlled. | | | | |
| 3 | Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. | | | | |
| 4 | Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system. | | | | |
| 5 | It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. | | | | |

| | **ISC Description - Communications and Operations Management** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 6 | The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly. | | | | |
| 7 | Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks. | | | | |
| 8 | The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. | | | | |
| 9 | Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. | | | | |
| 10 | Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. | | | | |
| 11 | Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing. | | | | |
| 12 | Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy. | | | | |

| | **ISC Description - Communications and Operations Management** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 13 | Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. | | | | |
| 14 | Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced. | | | | |
| 15 | There should be procedures in place for the management of removable media. | | | | |
| 16 | Media should be disposed of securely and safely when no longer required, using formal procedures. | | | | |
| 17 | Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse. | | | | |
| 18 | System documentation should be protected against unauthorized access. | | | | |
| 19 | Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. | | | | |
| 20 | Agreements should be established for the exchange of information and software between the organization and external parties. | | | | |
| 21 | Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries. | | | | |

| | **ISC Description - Communications and Operations Management** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 22 | Information involved in electronic messaging should be appropriately protected. | | | | |
| 23 | Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems. | | | | |
| 24 | Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. | | | | |
| 25 | Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. | | | | |
| 26 | Publicly available information: The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification. | | | | |
| 27 | Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. | | | | |
| 28 | Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. | | | | |
| 29 | Logging facilities and log information should be protected against tampering and unauthorized access. | | | | |

| | **ISC Description - Communications and Operations Management** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 30 | System administrator and system operator activities should be logged. | | | | |
| 31 | Faults should be logged, analyzed, and appropriate action taken. | | | | |
| 32 | The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Access Control

| | **ISC Description - Access Control** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | An access control policy should be established, documented, and reviewed based on business and security requirements for access. | | | | |
| 2 | There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. | | | | |
| 3 | The allocation and use of privileges should be restricted and controlled. | | | | |
| 4 | The allocation of passwords should be controlled through a formal management process. | | | | |
| 5 | Management should review users' access rights at regular intervals using a formal process. | | | | |

| | **ISC Description - Access Control** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 6 | Users should be required to follow good security practices in the selection and use of passwords. | | | | |
| 7 | Users should ensure that unattended equipment has appropriate protection. | | | | |
| 8 | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. | | | | |
| 9 | Users should only be provided with access to the services that they have been specifically authorized to use. | | | | |
| 10 | Appropriate authentication methods should be used to control access by remote users. | | | | |
| 11 | Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. | | | | |
| 12 | Physical and logical access to diagnostic and configuration ports should be controlled. | | | | |
| 13 | Groups of information services, users, and information systems should be segregated on networks. | | | | |
| 14 | For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications. | | | | |
| 15 | Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. | | | | |

| | ISC Description - Access Control | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC C**omplies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 16 | Access to operating systems should be controlled by a secure log-on procedure. | | | | |
| 17 | All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. | | | | |
| 18 | Systems for managing passwords should be interactive and should ensure quality passwords. | | | | |
| 19 | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | | | | |
| 20 | Inactive sessions should shut down after a defined period of inactivity. | | | | |
| 21 | Restrictions on connection times should be used to provide additional security for high-risk applications. | | | | |
| 22 | Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. | | | | |
| 23 | Sensitive systems should have a dedicated (isolated) computing environment. | | | | |
| 24 | A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities. | | | | |
| 25 | A policy, operational plans, and procedures should be developed and implemented for teleworking activities. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Information Systems Acquisition, Development, and Maintenance

| | **ISC Description - Information Systems Acquisition, Development, And Maintenance** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls. | | | | |
| 2 | Data input to applications should be validated to ensure that this data is correct and appropriate. | | | | |
| 3 | Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. | | | | |
| 4 | Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented. | | | | |
| 5 | Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. | | | | |
| 6 | A policy on the use of cryptographic controls for protection of information should be developed and implemented. | | | | |
| 7 | Key management should be in place to support the organization's use of cryptographic techniques. | | | | |
| 8 | There should be procedures in place to control the installation of software on operational systems. | | | | |
| 9 | Test data should be selected | | | | |

| | **ISC Description - Information Systems Acquisition, Development, And Maintenance** | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC C**omplies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| | carefully, and protected and controlled. | | | | |
| 10 | Access to program source code should be restricted. | | | | |
| 11 | The implementation of changes should be controlled by the use of formal change control procedures. | | | | |
| 12 | When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | | | | |
| 13 | Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled. | | | | |
| 14 | Opportunities for information leakage should be prevented. | | | | |
| 15 | Outsourced software development should be supervised and monitored by the organization. | | | | |
| 16 | Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Information Security Incident Management

| | ISC Description - Information Security Incident Management | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | Information security events should be reported through appropriate management channels as quickly as possible. | | | | |
| 2 | All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services. | | | | |
| 3 | Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. | | | | |
| 4 | There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. | | | | |
| 5 | Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Business Continuity Management

| | ISC Description - Business Continuity Management | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity. | | | | |
| 2 | Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. | | | | |
| 3 | Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. | | | | |
| 4 | A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. | | | | |
| 5 | Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

## Compliance

| | ISC Description - Compliance | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| 1 | All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. | | | | |
| 2 | Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. | | | | |
| 3 | Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. | | | | |
| 4 | Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. | | | | |
| 5 | Users should be deterred from using information processing facilities for unauthorized purposes. | | | | |
| 6 | Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. | | | | |
| 7 | Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. | | | | |
| 8 | Information systems should be regularly checked for compliance with security implementation | | | | |

| | ISC Description - Compliance | **Estimated Implementation Cost (in thousands) **** | **Scope** - Number of systems/applications protected by ISC. [**1, More than 1**] | Extent to which the ISC **Complies** with required, external laws and regulations [**0 - 100%**] | Extent to which the ISC addresses information security **risks** [**0 - 100%**] |
|---|---|---|---|---|---|
| | standards. | | | | |
| 9 | Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. | | | | |
| 10 | Access to information systems audit tools should be protected to prevent any possible misuse or compromise. | | | | |

** An EIC of $0 implies that the ISC can be performed by *existing* system resources or *existing* resource personnel as part of their daily responsibilities.

# Appendix B. Experts' Interviews and Calls

Legend:
AC - Access Control
C - Compliance
HRS - Human Resource Security
P.I. - Personal Interview
P.C. - Phone Call

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 11/7/2013 | AC-1 Security parameters are not adequately configured, allowing for potential unauthorized user access to financially significant systems, applications, or databases. | 1 | | √ | 8:00 AM | 8:30 AM | 0:30 | Yes | "FST generated ISC 6, which prompts users to select and use good passwords, as well as ISC 16 to control access to systems via secure logons. Both of these controls address this risk." |
| 2 | 11/7/2013 | AC-1 Security parameters are not adequately configured, allowing for potential unauthorized user access to financially significant systems, applications, or databases. | 2 | | √ | 5:00 PM | 6:00 PM | 1:00 | Yes | "To prevent unauthorized access, the new methodology resulted in ISC 3, ISC 5, and ISC 9, all relating to the control, review, and assignment of adequate access." |
| 3 | 11/8/2013 | AC-1 Security parameters are not adequately configured, allowing for potential unauthorized user access to financially significant systems, applications, or databases. | 3 | √ | | 10:00 AM | 11:00 AM | 1:00 | Yes | "The controls ISC 6, ISC 10, and ISC 17 selected by the FST methodology help in mitigating this risk. Also, there are other selected controls like ISC 5 that can deal with the issue of unauthorized access." |
| 4 | 11/11/2013 | AC-2 Privileges are granted to users which are not consistent with their job functions. The above allows unauthorized or incorrect modifications to financial data, resulting in segregation of duties conflicts, unprevented or undetected errors, incorrect financials, and/or management decisions based upon misleading information. | 1 | | √ | 8:00 AM | 8:45 AM | 0:45 | Yes | "ISC 3 calls for the control and restriction of privileges, while ISC 5 reviews user access. ISC 9 further states that users should only be provided access to the services they are responsible for and have been authorized to use. The combination of these three controls addresses this risk." |
| 5 | 11/11/2013 | AC-2 Privileges are granted to users which are not consistent with their job functions. The above allows unauthorized or incorrect modifications to financial data, resulting in segregation of duties conflicts, unprevented or undetected errors, incorrect financials, and/or management | 2 | | √ | 2:00 PM | 3:00 PM | 1:00 | Yes | "The FST methodology prompted the selection of ISC 3 and ISC 9. ISC 3 restricts access and ISC 9 ensures that access must be authorized and granted only to the services and responsibilities users need. Both of these controls address the RISR." |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| | | decisions based upon misleading information. | | | | | | | | |
| 6 | 11/11/2013 | AC-3 Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information. | 1 | | √ | 9:00 AM | 9:30 AM | 0:30 | Yes | "Selection of ISC 5 takes care of this risk." |
| 7 | 11/11/2013 | AC-3 Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information. | 2 | | √ | 3:00 PM | 4:00 PM | 1:00 | Yes | "ISC 5 relates to the periodic reviews of user access rights by Management. Frequent reviews of user access ensure, for example, that terminated user accounts do not gain access to financial systems or data. Additionally, ISC 1 (also selected by FST) prompts for the establishment of a policy to guide access control." |
| 8 | 11/13/2013 | AC-2 Privileges are granted to users which are not consistent with their job functions. The above allows unauthorized or incorrect modifications to financial data, resulting in segregation of duties conflicts, unprevented or undetected errors, incorrect financials, and/or management decisions based upon misleading information. | 3 | √ | | 6:00 PM | 6:30 PM | 0:30 | Yes | "Controls ISC 3, ISC 5, and ISC 9 address this RISR. These controls were selected by the FST methodology. In addition, ISC 1, which talks about the need of an access control policy, is also a good control to address this risk since implementation of such type of control sets the right tone at the top." |
| 9 | 11/13/2013 | AC-3 Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information. | 3 | √ | | 6:30 PM | 7:00 PM | 0:30 | Yes | "The combination of ISC5 and ISC 20, both selected by the FST methodology, in my opinion, help address this RISR. ISC 5 requires management reviews of access to be performed at regular intervals. This will most likely detect accounts (terminated, for example) that should not be active. At the same time, ISC 20 relates to shutting down inactive sessions, which is also required for terminated accounts." |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 11/13/2013 | AC-4 Users with unauthorized accounts can change configuration settings or execute system administration activities to financial applications' parameters, giving rise to potential fraud, invalid data, failure to safeguard assets, or misled management. | 3 | √ | | 7:00 PM | 8:00 PM | 1:00 | Yes | "The FST methodology suggested the selection of ISC 16, which requires secure log-on procedures to access operating systems (including access to their system functions, configuration settings, etc.). Moreover, ISC 19 (also suggested for selection) restricts access to utility programs which can impact, in a negative way, current systems and application settings, controls, etc. Lastly, an access control policy should be established to include the controls and procedures just mentioned. All these controls put in place address the RISR." |
| 11 | 11/15/2013 | AC-4 Users with unauthorized accounts can change configuration settings or execute system administration activities to financial applications' parameters, giving rise to potential fraud, invalid data, failure to safeguard assets, or misled management. | 1 | | √ | 8:00 AM | 8:20 AM | 0:20 | Yes | "The selected control ISC 22 restricts access to system functions, including, configuration settings, systems' and applications' parameters within applications, thereby, taking care of this risk." |
| 12 | 11/15/2013 | C-1 Breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements take place over the design, operation, use, and management of information systems. | 1 | | √ | 8:20 AM | 9:10 AM | 0:50 | Yes | "The tool selected ISC 1, which requires explicit definitions of 'all relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements'. Establishment of these requirements will serve well in addressing this risk." |
| 13 | 11/18/2013 | AC-4 Users with unauthorized accounts can change configuration settings or execute system administration activities to financial applications' parameters, giving rise to potential fraud, invalid data, failure to safeguard assets, or misled management. | 2 | | √ | 10:30 AM | 11:15 AM | 0:45 | Yes | "Utility programs that can override system and application controls should be restricted and controlled, which is the purposes of ISC 19. A defined access control policy, as required by ISC 22, will further restrict access to system functions within applications. The 2 controls just mentioned address this RISR." |
| 14 | 11/20/2013 | C-1 Breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements take place over the | 2 | | √ | 4:00 PM | 4:30 PM | 0:30 | Yes | "Verifying systems and applications regularly for compliance (ISC 8), as well as having a clear definition of all relevant statutory, regulatory, and |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| | | design, operation, use, and management of information systems. | | | | | | | | contractual requirements (ISC 1), both, should address the RISR in question." |
| 15 | 11/23/2013 | C-1 Breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements take place over the design, operation, use, and management of information systems. | 3 | √ | | 4:00 PM | 4:40 PM | 0:40 | Yes | "The FST methodology suggested the selection of ISC 1 ('All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.'), a critical step in addressing this RISR. Further, and combined with the above, checking information systems, applications, etc. periodically for compliance with obligations (regulatory, statutory, contractual, etc.) (control ISC 8) will also address the risk, as well as strengthen current compliance procedures at the Organization." |
| 16 | 11/23/2013 | C-2 Information systems are not in compliance with organizational security implementation policies, standards, and documented security controls. | 3 | √ | | 4:50 PM | 5:20 PM | 0:30 | Yes | "The selection of controls ISC 1 and ISC 8 by the new methodology ensures the RISR in question is addressed. ISC 1, for instance, mandates that significant requirements (statutory, regulatory, and contractual) be defined and documented so that they can be complied with. Equally important and to add to ISC 1, periodic checks for compliance with statutory, regulatory, and contractual requirements must occur consistent with control ISC 8." |
| 17 | 11/23/2013 | C-3 Operational systems and audit tools are not adequately safeguarded to prevent their misuse. | 3 | √ | | 5:25 PM | 6:05 PM | 0:40 | Yes | "The FST methodology suggested the selection of ISC 9 to monitor operational systems' activities to reduce disruptions to business processes. ISC 10, also selected by the methodology, calls for access protection of information systems audit tools, again, to avoid any possible misuse, compromise, etc. These two ISC's address the RISR." |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| 18 | 11/25/2013 | C-2 Information systems are not in compliance with organizational security implementation policies, standards, and documented security controls. | 2 | | √ | 9:00 AM | 9:35 AM | 0:35 | Yes | "ISC 1 calls for the establishment, definition, and compliance of information systems with 'all relevant statutory, regulatory, and contractual requirements...', thereby, addressing this RISR." |
| 19 | 11/25/2013 | C-3 Operational systems and audit tools are not adequately safeguarded to prevent their misuse. | 2 | | √ | 9:35 AM | 10:30 AM | 0:55 | Yes | "The requirement for protection of information systems and audit tools to avoid misuses, etc., stated by the selected ISC 10, addresses the RISR." |
| 20 | 11/26/2013 | C-2 Information systems are not in compliance with organizational security implementation policies, standards, and documented security controls. | 1 | | √ | 8:00 AM | 8:35 AM | 0:35 | Yes | "ISC 8, selected, states that information systems should be regularly checked for compliance with security implementation standards. Such control, on its own, addresses this risk." |
| 21 | 11/26/2013 | C-3 Operational systems and audit tools are not adequately safeguarded to prevent their misuse. | 1 | | √ | 8:35 AM | 9:00 AM | 0:25 | Yes | "ISC 9 and ISC 10 require procedures to be performed on operating systems and audit tools to keep them functional and protected, respectively. Both address this risk directly." |
| 22 | 11/30/2013 | HRS-1 Employees, contractors, and third party users do not understand their responsibilities, and are not suitable for the roles they are considered for. | 3 | √ | | 3:00 PM | 4:00 PM | 1:00 | Undecided | N/A |
| 23 | 12/3/2013 | HRS-1 Employees, contractors, and third party users do not understand their responsibilities, and are not suitable for the roles they are considered for. | 1 | | √ | 8:00 AM | 8:55 AM | 0:55 | Yes | "ISC 1 responds solidly to this risk by defining all security roles and responsibilities of employees, etc." |
| 24 | 12/3/2013 | HRS-1 Employees, contractors, and third party users do not understand their responsibilities, and are not suitable for the roles they are considered for. | 2 | | √ | 11:00 AM | 11:55 AM | 0:55 | Undecided | N/A |
| 25 | 12/6/2013 | HRS-2 The risk of theft, fraud or misuse of facilities is not reduced. | 1 | | √ | 7:30 AM | 8:20 AM | 0:50 | No | "To reduce the risk of theft, fraud or misuse of facilities, ISC 6 (enforcement of a 'formal disciplinary process for employees who have committed a security breach') should have been selected, but it wasn't. Luckily, this ISC was already implemented by the Organization." |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| 26 | 12/6/2013 | HRS-2 The risk of theft, fraud or misuse of facilities is not reduced. | 2 | | √ | 1:00 PM | 1:40 PM | 0:40 | No | "There is no current process for reprimanding users when faulting or committing security breaches (required by ISC 6). Because of that, ISC 6 should have been selected." |
| 27 | 12/7/2013 | HRS-2 The risk of theft, fraud or misuse of facilities is not reduced. | 3 | √ | | 10:00 AM | 11:00 AM | 1:00 | No | "The FST methodology did not select ISC 6, which targets this RISR via the establishment of a disciplinary process." |
| 28 | 12/7/2013 | HRS-3 Security responsibilities related to job descriptions and conditions of employment are not necessarily addressed prior to employment. | 1 | | √ | 4:00 PM | 4:30 PM | 0:30 | No | "ISC 3 should have been selected to properly address employees' understanding of security responsibilities, which refers to the risk here." |
| 29 | 12/11/2013 | HRS-1 Employees, contractors, and third party users do not understand their responsibilities, and are not suitable for the roles they are considered for. | 2 | | √ | 11:30 AM | 12:30 PM | 1:00 | No | Undecided on 12/3/2013. "To address this RISR, users should receive appropriate training, relevant for their job function, as well as agree by signing the terms, conditions, and responsibilities they were hired for. The requirements just mentioned are stated in ISC 3 and ISC 5, respectively, both controls not selected by the tool. The RISR is not addressed." |
| 30 | 12/12/2013 | HRS-1 Employees, contractors, and third party users do not understand their responsibilities, and are not suitable for the roles they are considered for. | 3 | √ | | 6:00 PM | 7:00 PM | 1:00 | No | Refer to previous meeting held on 11/30/2013. "Even though ISC 1 was selected by the FST methodology prompting for the definition and documentation of security roles and responsibilities for all employees, ISC 3 and ISC 5, both dealing directly with this RISR, were not selected. Awareness trainings represent a critical step for organizations to provide new and existing employees relevant information regarding organizational policies, procedures, and responsibilities of the job function (ISC 5). Proof of training participation and understanding of the material covered must be obtained and evidenced through formal, signed agreements from employees, contractors, |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | and third party users." |
| 31 | 12/14/2013 | HRS-3 Security responsibilities related to job descriptions and conditions of employment are not necessarily addressed prior to employment. | 3 | √ | | 10:30 AM | 10:55 AM | 0:25 | No | "The FST methodology did not select ISC 3, which requires formal agreement of the employee and his or her new contractual obligation, as well as organization's responsibilities specific to information security. In addition, prior to employment, background verification checks should be enforced and performed on all potential employees consistent with relevant laws, regulations, and ethics (said control refers to the unselected ISC 2). I understand that the RISR was not addressed." |
| 32 | 12/14/2013 | HRS-4 All candidates for employment, contractors, and third party are not adequately screened, especially for sensitive jobs. | 3 | √ | | 11:00 AM | 11:50 AM | 0:50 | No | "ISC 2 deals with performing background verification checks as part of the screening process on potential employees. Such control was not selected. ISC 3, on the other hand, and similar to my previous comment, was also not selected by the FST methodology. ISC 3 requires agreement between the organization and the employee in terms of their understanding of information security prior to employment. The absence of these 2 controls renders the RISR, in my opinion, not addressed." |
| 33 | 12/14/2013 | HRS-5 Employees, contractors, and third party users are (1) not aware of information security threats and concerns, their responsibilities and/or liabilities; and (2) not equipped to support organizational security policy in the course of their normal work, and | 3 | √ | | 1:20 PM | 2:00 PM | 0:40 | No | "The already-selected ISC 1 talks about defining security roles and responsibilities for employees, contractors, third party, etc. to assist them in understanding information security threats and concerns, etc. However, such understanding should |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| | | to reduce the risk of human error. | | | | | | | | be refreshed periodically via awareness trainings (purpose of ISC 5). Having awareness trainings and regular updates in organizational policies and procedures, for example, was not one of the controls selected by the FST tool. As such, the RISR is not addressed." |
| 34 | 12/17/2013 | HRS-3 Security responsibilities related to job descriptions and conditions of employment are not necessarily addressed prior to employment. | 2 | | √ | 9:00 AM | 9:30 AM | 0:30 | No | "ISC 3 requires formal agreement (evidenced by a signoff) between employees and the organization in regards to the terms and conditions of the employment contract, including and, more importantly, their responsibilities in terms of information security. The selection of this control alone should have addressed the RISR." |
| 35 | 12/17/2013 | HRS-4 All candidates for employment, contractors, and third party are not adequately screened, especially for sensitive jobs. | 1 | | √ | 3:30 PM | 4:00 PM | 0:30 | No | "Screenings of candidates via background verification checks, for instance, are required by ISC 2, which was not one of the controls selected. Thus, this risk is not mitigated." |
| 36 | 12/18/2013 | HRS-4 All candidates for employment, contractors, and third party are not adequately screened, especially for sensitive jobs. | 2 | | √ | 9:45 AM | 10:20 AM | 0:35 | No | "The methodology did not prompt ISC 2 for selection. ISC 2 requires background checks, screenings to be performed on potential employees, particularly when considered for critical and sensitive jobs." |
| 37 | 1/3/2014 | HRS-5 Employees, contractors, and third party users are (1) not aware of information security threats and concerns, their responsibilities and/or liabilities; and (2) not equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. | 1 | | √ | 7:30 AM | 8:40 AM | 1:10 | No | "Even though control ISC 1 (definition of security roles and responsibilities) was selected, ISC 5 (awareness trainings) was not. The organization should implement both, ISC1 and ISC5, to strengthen its security." |
| 38 | 1/3/2014 | HRS-6 An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities is not provided to all employees, contractors and third party users to minimize possible security risks. | 1 | | √ | 8:40 AM | 9:20 AM | 0:40 | No | "Control ISC 5 was not selected; risk is not addressed." |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| 39 | 1/6/2014 | HRS-5 Employees, contractors, and third party users are (1) not aware of information security threats and concerns, their responsibilities and/or liabilities; and (2) not equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. | 2 | √ | | 3:00 PM | 4:05 PM | 1:05 | No | "Awareness of security threats, concerns, responsibilities, etc. at organizations comes from having an adequate training or seminar program in place. This is suggested by ISC 5, which was not selected by the tool. As a result, the RISR is not addressed." |
| 40 | 1/6/2014 | HRS-6 An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities is not provided to all employees, contractors and third party users to minimize possible security risks. | 2 | √ | | 5:00 PM | 6:00 PM | 1:00 | No | "ISC 5 deals with this RISR directly and such control was not selected by the tool, leaving the RISR unaddressed. Fortunately, this control had been in place by the organization. The organization should continue performing this control." |
| 41 | 1/8/2014 | HRS-7 A formal disciplinary process for handling security breaches is not established. | 1 | | √ | 7:30 AM | 8:00 AM | 0:30 | No | "Control ISC 6 was not selected; risk is not addressed." |
| 42 | 1/8/2014 | HRS-8 The exit process for employees, contractors, and third party is not performed effectively or in a timely or orderly manner. Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed. | 1 | | √ | 8:00 AM | 8:40 AM | 0:40 | Yes | "Selection of controls ISC 7 and ISC 9, both related to termination access and procedures, will address this risk." |
| 43 | 1/10/2014 | HRS-7 A formal disciplinary process for handling security breaches is not established. | 2 | | √ | 4:00 PM | 4:40 PM | 0:40 | No | "ISC 6 was not selected, so no formal disciplinary process is required to be in place at the organization." |
| 44 | 1/10/2014 | HRS-8 The exit process for employees, contractors, and third party is not performed effectively or in a timely or orderly manner. Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed. | 2 | | √ | 4:45 PM | 5:25 PM | 0:40 | Undecided | N/A |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| 45 | 1/11/2014 | HRS-6 An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities is not provided to all employees, contractors and third party users to minimize possible security risks. | 3 | √ | | 11:00 AM | 11:40 AM | 0:40 | No | "Again, ISC 5 was not selected by the new methodology; therefore, the RISR is not addressed. Nevertheless, control ISC 5 was already part of the ISC's in place at the organization. This is an example where controls already implemented at the organization plus the ones selected by FST, when combined, can strengthen information security." |
| 46 | 1/11/2014 | HRS-7 A formal disciplinary process for handling security breaches is not established. | 3 | √ | | 1:15 PM | 1:50 PM | 0:35 | No | "The methodology did not select ISC 6, which deals specifically with having a disciplinary process in case of security breaches, etc. Although the RISR is not addressed, the organization had this control in place prior to running the FST methodology. This is another example where the organization should continue with its previous control to continue having a proper level of security around this area." |
| 47 | 1/11/2014 | HRS-8 The exit process for employees, contractors, and third party is not performed effectively or in a timely or orderly manner. Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed. | 3 | √ | | 2:00 PM | 2:25 PM | 0:25 | No | "To address the RISR of not performing an effective, timely, and ordered exit meeting process, control ISC 8 (requiring employees to return all organization's equipment upon termination) should have been chosen by the FST methodology." |
| 48 | 1/11/2014 | HRS-9 Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information. | 3 | √ | | 2:25 PM | 3:00 PM | 0:35 | Yes | "The methodology chose ISC 7, which requires all responsibilities related to employment termination to be clearly defined and assigned. In addition, ISC 9, requires the removal of access for all accounts upon termination. Both selected controls address the RISR." |

| | Date | Relevant Information Security Risk ("RISR") | Expert # | P.I. | P.C. | Time Start | Time End | Duration | Risk Addressed? | Comments Summarizing Risk Determination |
|---|---|---|---|---|---|---|---|---|---|---|
| 49 | 1/15/2014 | HRS-8 The exit process for employees, contractors, and third party is not performed effectively or in a timely or orderly manner. Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed. | 2 | | √ | 10:00 AM | 11:05 AM | 1:05 | Yes | "Undecided at 1/10/2014 given that ISC 8 had not been selected by the tool. However, the combination of selected controls ISC 7 and ISC 9, both stating responsibilities when dealing with terminations, in my opinion, address the RISR." |
| 50 | 1/15/2014 | HRS-9 Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information. | 2 | | √ | 11:15 AM | 11:50 AM | 0:35 | Yes | "ISC 9 prevents terminated users from gaining unauthorized access to financial systems (which refers to this RISR) by prompting the removal of access of all such terminated employees, contractors, and third party users." |
| 51 | 1/16/2014 | HRS-9 Users with terminated accounts as well as other unauthorized users can gain access to financial systems or data, and view and/or change critical, confidential, or sensitive financial information. | 1 | | √ | 8:00 AM | 8:45 AM | 0:45 | Yes | "Control ISC 9, selected, addresses this risk." |
| | | **Total Personal Interviews, Phone Calls, and Duration** | | 19 | 32 | | | 12:55 | | |

# References

Aalst, W., & Kumar, A. (2003). XML-based schema definition for support of interorganizational workflow. *Information Systems Research, 14*(1), 23-46.

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

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

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

Bedard, J. C., Graham, L., & Jackson, C. (2008). Archival evidence on detection and severity classification of Sarbanes-Oxley Section 404 internal control deficiencies. Working paper, Bentley University.

Bhoyar, K. K., & Kakde, O. G. (2009). Image Retrieval using Fuzzy and Neuro-Fuzzy Approaches with Fuzzy Color Semantics. *International Conference on Digital Image Processing*, 39-44.

Biery, K. (2006). Aligning an information risk management approach to BS 7799-3:2005. SANS Institute, InfoSec Reading Room.

Bowman, W. (2009), The economic value of volunteers to nonprofit organizations. *Nonprofit Management and Leadership, 19*(4), 491-506.

Cabaniss, K. (2001). Counseling and computer technology in the new millennium: An Internet Delphi study. *Digital Abstracts International*, *62*(1), 87.

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

Cheney, J. S., Hunt, R. M., Jacob, K., Porter, R. D., & Summers, B. J. (2012) *The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches* (October 2012). FRB of Philadelphia - Payment Cards Center Discussion Paper No. 12-04. Available at SSRN: http://ssrn.com/abstract=2162536 or http://dx.doi.org/10.2139/ssrn.2162536

Cox, E. (2005). *Fuzzy modeling and genetic algorithms for data mining and exploration.* Amsterdam, Boston: Elsevier/Morgan Kaufmann.

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

Das, P. (2009). Adaptation of fuzzy reasoning and rule generation for customers' choice in retail FMCG business. *Journal of Management Research, 9*(1), 15-15-26.

Demicco, R. V., & Klir, G. J. (2004). *Fuzzy logic in geology*. Academic Press.

Denning, P. J. (1997). A new social contract for research. *Communications of the ACM, 40*(2), 132-134.

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

Ejnioui, A., Otero, A. R., Tejay, G., Otero, C. E., & Qureshi, A. "A Multi-Attribute Evaluation of Information Security Controls in Organizations Using Grey Systems Theory" to appear in *International Conference on Security and Management*, 2012.

Emory, C. W., & Cooper, D. R. (1991). *Business Research Methods*. Irwin, Boston, MA.

FBI, Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Years 2007 through 2011, Department of Justice, United States, http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011

FBI, Federal Bureau of Investigation, Financial Crimes Report to the Public Fiscal Year, Department of Justice, United States, 2009, http://www.fbi.gov/stats-services/publications/financial-crimes-report-2009/financial-crimes-report-2009#corporate

Fontela, E., & Gabus, A. (1976). *The DEMATEL observer*. Battelle Institute, Geneva Research Center.

Gabus, A., & Fontela, E. (1972). *World problems an invitation to further thought within the framework of DEMATEL*. Battelle Geneva Research Centre, Geneva, Switzerland.

Genske, D. D., & Heinrich, K. (2009). A knowledge-based fuzzy expert system to analyze degraded terrain. *Expert Systems with Applications, 36*, 2459-2472.

Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security, 27*(5), 124-135. doi:10.1016/j.cose.2008.07.009.

Gordon, L., & Loeb, M. (2006). Budgeting process for information security expenditure, *Communications of the ACM, 29*(1), 121-126.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

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

Huang, S. M., Hung, W. H., Yen, D. C., Chang, I., & Jiang, D. (2011). Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems*, *50*(4), 692-701.

Kantšukov, M., Medvedskaja, D. (2013), From Dishonesty to Disaster: The Reasons and Consequences of Rogue Traders' Fraudulent Behavior, in Tiia Vissak, Maaja Vadi (ed.) *(Dis)Honesty in Management (Advanced Series in Management, Volume 10)*, Emerald Group Publishing Limited, pp.147-165. DOI: 10.1108/S1877-6361(2013)0000010011

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2004). Information systems security policies: A contextual perspective. *Computer Security, 24*(1), 246-260.

Kaur, A., & Kaur, A. (2012). Comparison of mamdani-type and sugeno-type fuzzy inference systems for air conditioning system. *International Journal of Soft Computing and Engineering, 2*(2), 323-325.

Klir, G. J., & Yuan, B. (1995). *Fuzzy sets and logic: Theory and applications.* Prentice Hall PTR.

Larsen, P. M. (1980). Industrial applications of fuzzy logic control. *International Journal of Man-Machine Studies, 12*(1), 3-10.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical research* (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall.

Liou, J. J. H., Tzeng, G. H., & Chang, H. C. (2007). Airline safety measurement using a hybrid model. *Air Transport Management, 13*(4), 243-249.

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

Lorterapong, P. (1995). *Fuzzy Project-Network Scheduling Under Resource Constraints*. Concordia University. Montreal, Quebec, Canada.

Lv, J.-L., Zhou, Y.-S., & Wang, Y. Z. (2011). A multi-criteria evaluation method of information security controls. *Fourth International Joint Conference on Computational Sciences and Optimization*, 190-194.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. New York, NY: O'Reilly.

Mizumoto, M., & Zimmermann, H. J. (1982). Comparison of fuzzy reasoning methods. *Fuzzy Sets and Systems, 8*(3), 253-283.

Nunamaker, J., Chen, M., & Purdin, T. D. M. (1991a). Systems development in information systems research. *Journal of Management Information Systems, 7*(3), 89-106.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*(1), 15-29.

Opricovic, S., & Tzeng, G. H. (2007). Extended VIKOR method in comparison with outranking methods. *European Journal of Operational Research, 178*(2), 514-529.

Otero, A. R., Ejnioui, A., Otero, C. E., & Tejay, G. (2012a). Evaluation of information security controls in organizations by grey relational analysis. *International Journal of Dependable and Trustworthy Information Systems,* in press.

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.

Otero, L. D., & Otero, C. E. (2011). A fuzzy expert system architecture for capability assessments in skill-based environments. *Expert Systems with Applications, 39*(1), 654-662.

Otero, A. R., Tejay, G., Otero, L. D., & Ruiz, A. (2012b). A fuzzy logic-based information security control assessment for organizations. *IEEE Conference on Open Systems,* 2012.

Ou Yang, Y. P., Shieh, H. M., & Tzeng, G. H. (2011). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences.* doi:10.1016/j.ins.2011.09.012

Ou Yang, Y. P., Shieh, H. M., Leu, J. D., & Tzeng, G. H. (2008). A novel hybrid MCDM model combined with DEMATEL and ANP with applications. *International Journal of Operations Research, 5*(3), 160-168.

Public Company Accounting Oversight Board (PCAOB). (2013, October 12). Auditing Standard – Identifying and Assessing Risks of Material Misstatement. Retrieved from

http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_12_Appendix_B.aspx.

Pedrycz, W. (1994). Why triangular membership functions? *Fuzzy Sets and Systems, 64*(1), 21-30.

Petrovic-Lazarevic, S. (2001). Personnel Selection Fuzzy Model. *International Transactions in Operational Research, 8*(1), 89-105.

Peirce, C. S. (1931). *Collected Papers*. Harshorne, C. and P. Weiss, Eds. Harvard University Press, Cambridge, MA.

Richards, J. E. (2000). Public health informatics: A consensus on core competencies. *Digital Abstracts International, 61*(8), 2964. (UMI No. 9983325)

Ross, T. J. (2010). *Fuzzy Logic with Engineering Applications* (3rd ed.). Chichester, UK: John Wiley & Sons, Inc.

Ross, T. J., Hassanein, H., & Ali, A. N. (2010). *Fuzzy logic with engineering applications: Design and stability analysis* (3rd ed.). Chichester, UK: John Wiley & Sons, Inc.

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

Saaty, T. L. (1996). *Decision Making with Dependence and Feedback: Analytic Network Process*. RWS Publications, Pittsburgh.

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

Salkind, N. J. (2009). *Exploring research* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Salmasi, F. R. (2007). Control Strategies for Hybrid Electric Vehicles: Evolution, Classification, Comparison, and Future Trends. *IEEE Transactions on Vehicular Technology, 56*(5), 2393-2404.

Schmidt, V. V. (1995). Awakening intuition: A Delphi study. *Digital Abstracts International, 56*(9), 3498. (UMI No. 9543808)

Schryen, G. (2010). A fuzzy model for IT security investments. In: Proceedings of Sicherheit, Schutz und Zuverlässigkeit, October 5-7, 2010, Berlin.

Sekaran, U. (2003). *Research methods for business: A skill building approach* (4th ed.). New York, NY: John Wiley & Sons, Inc.

Simon, H. A. (1996). *The sciences of the artificial* (3rd ed.). Cambridge, MA: MIT Press.

Siougle, E. S., & Zorkadis, V. C. (2002). A Model Enabling Law Compliant Privacy Protection through the Selection and Evaluation of Appropriate Security Controls. *Computer Science, 2437*, 104-114. doi: 10.1007/3-540-45831-X_8

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education, 6*(2007), 1-21.

Straub, D. W. (1986). Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment. *Dissertation Abstracts International, 48*(04), 813.

Tichy, W. (1998). Should computer scientists experiment more? *IEEE Computer, 31*(5), 32-40.

Tsichritzis, D. (1998). The dynamics of innovation. In P. J. Denning & R. M. Metcalfe (Eds.), *Beyond calculation: The next fifty years of computing* (pp. 259-265). New York, NY: Copernicus Books.

Tucker, S., Chmiel, N., Turner, N., Hershcovis, M. S., & Stride, C. B. (2008). Perceived organizational support for safety and employee safety voice: The mediating role of coworker support for safety. *Journal of Occupational Health Psychology, 13*(4), 319.

Tzeng, G. H., Chiang, C. H., & Li, C. W. (2007). Evaluating intertwined effects in e-learning programs: a novel hybrid MCDM model based on factor analysis and DEMATEL. *Expert Systems with Applications, 32*(4), 1028-1044.

Vaishnavi, V., & Kuechler, W. (2004). Design science research in information system. Retrieved from http://desrist.org/desrist

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

Wang, H., Xu, H., Chan, H. C., & Chen, L. (2002). Critical success factors for Web-based organizational IT training systems. In Advances in Web-Based Learning (pp. 142-153). Springer Berlin Heidelberg.

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.

Yaakob, S. B., & Watada, J. (2009, August). Fuzzy approach for assignment problem. In *Fuzzy Systems, 2009. FUZZ-IEEE 2009. IEEE International Conference on* (pp. 1408-1413). IEEE.

Yager, R. R. (1996). Knowledge-based defuzzification. *Fuzzy Sets Systems, 80*(1), 177-185.

Zadeh, L. (1965). Fuzzy sets. *Information Control, 8*(1), 338-353.

Zelkowitz, M., & Wallace, D. (1998). Experimental models for validating technology. *IEEE Computer, 31*(5), 23-31.

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

Zimmermann H-J. (2001). *Fuzzy Set Theory—and Applications*, 4th Rev. ed. Boston: Kluwer Academic Publishers; 2001.

Zlateva, P., Velev, D., & Zabunov, G. (2011). A model for fuzzy logic assessment of real estate investment risks. *Advances in Intelligent and Soft Computing, 101*(1), 89-93. doi: 10.1007/978-3-642-23163-6_13

Zmud, R. (1997). "Editor's Comments," MIS Quarterly (21:2), June 1997, pp. xxi-xxii.