2008

Developing a Multi-Objective Decision Model for Maximizing IS Security within an Organization

Jeffrey Lee May
Virginia Commonwealth University

DEVELOPING A MULTI-OBJECTIVE DECISION MODEL FOR MAXIMIZING IS SECURITY WITHIN AN ORGANIZATION

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business with Major in Information Systems at Virginia Commonwealth University

by

JEFFREY LEE MAY
BS, Mechanical Engineering, Wright State University, 1993
MS, Environmental Engineering, Virginia Tech, 1996
MS, Information Systems, Virginia Commonwealth University, 2003

Dissertation Chair: Dr. Gurpreet Dhillon
Professor, Information Systems
Virginia Commonwealth University

Virginia Commonwealth University
Richmond, VA
May, 2008

Acknowledgement

This dissertation would not have been completed without the loving support of my beautiful wife, Valarie. She continued her support through many restless nights and months of aggravating days and has taught me the true meaning of unconditional love. Thank you, Valarie. I love you very much!

I would also like to thank my five committee members from Virginia Commonwealth University. First, I would like to thank Dr. Gurpreet Dhillon, my advisor and dissertation chair, for his continued support and advice along with providing me with a theoretical template from which to begin this work. I look forward to our continued relationship as both colleagues and friends. Second, I would like to thank Dr. Richard Redmond for his wonderful advice and for providing me with an instructor position at VCU while I worked on my Ph.D. Third, I would like to thank Dr. Carolyn Strand Norman for providing me with the connection to the organization that was studied in this research and for giving me both academic and emotional support. Fourth, I would like to thank Dr. George Kasper for providing me with excellent behind-the-scenes advice but more importantly, for his unique ability to keep a smile on my face. And finally, I would like to thank Dr. Jason Merrick for providing me with the conceptual foundation used for handling the methodological aspects of this research.

I would also like to thank Dr. Richard Mathieu at James Madison University for providing me with the necessary motivation and advice to finish this dissertation and for hiring me as a faculty member at JMU. And last but not least, I would like to thank Tina

Babb, the Business Manager at Virginia Commonwealth University, for always being there when I needed a friend!

Table of Contents

List of Tables

List of Figures

List of Acronyms and Reoccurring Names

MODA	Multiple Objective Decision Analysis
IS	Information System
DM	Decision Maker
RM	Risk Management
DOD	Department of Defense
AFT	Alternative Focused Thinking
VFT	Value-Focused Thinking
CIA	Confidentiality, Integrity of Data, Availability
RITE	Responsibility, Integrity of Roles, Trust, Ethicality
WITI	Why Is That Important
SDVF	Single-Dimensional Value Function
AHP	Analytic Hierarchy Process
MSI Corp.	Fictitious name of the organization that took part in this research
Team	Name used to refer to the three respondents who took part in this research

Abstract

DEVELOPING A MULTI-OBJECTIVE DECISION MODEL FOR MAXIMIZING IS SECURITY WITHIN AN ORGANIZATION

By Jeffrey Lee May, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business with Major in Information Systems at Virginia Commonwealth University

Virginia Commonwealth University, 2008

Dissertation Chair: Dr. Gurpreet Dhillon
Professor, Department of Information Systems

Numerous IS researchers have argued that IS Security can be more effectively managed if the emphasis goes beyond the technical means of protecting information resources. In an effort to adopt a broader perspective that accounts for issues that transcend technical means alone, Dhillon and Torkzadeh (2006) present an array of 9 fundamental and 16 means objectives that are essential for maximizing IS security in an organization. These objectives were derived using a value-focused thinking approach and are organized into a conceptual framework. This conceptual framework provides a rigorous theoretical base for considering IS security in a manner that accounts for both technical and organizational issues; however, no direction is provided for using these objectives so that informed decisions can be made. As a result, the goal of this dissertation is to develop a decision model using Multiple Objective Decision Analysis

(MODA) techniques that seek to provide informed alternatives to decision makers who desire to maximize IS security within an organization.

Chapter 1 - Orientation

1.1 Introduction

Information system (IS) security continues to present a major challenge to organizations. Currently, a number of traditional techniques are being used that attempt to provide a means for assessing and thus improving IS security. However, these traditional techniques have been shown to concentrate solely on technical matters such as confidentiality, integrity, and availability of data (CIA). Yet, numerous IS researchers have argued that IS security can be more effectively managed if the emphasis goes beyond the technical means of protecting information resources (Baskerville, 1993; Hitchings, 1996; Segev et al., 1998; Straub and Welke, 1998; Armstrong, 1999; Dhillon and Backhouse, 2001; Dhillon and Torkzadeh, 2006). This new emphasis has been labeled as the socio-organizational approach (Dhillon and Backhouse, 2001) to IS security where constructs such as ethical practices, cultural sensitivity, responsibility and awareness are considered along with the traditional constructs of CIA.

In an effort to identify IS security constructs from the socio-organizational perspective, Dhillon and Torkzadeh (2006) present an array of 9 fundamental and 16 means objectives[1] that are essential for maximizing IS security in an organization. These objectives were derived using Keeney's (1992) value-focused thinking approach and are organized into a conceptual framework. This conceptual framework provides a rigorous

[1] These objectives are shown in Tables 2.1 and 2.2 in Chapter 2.

theoretical base for considering IS security in a manner that accounts for both technical and organizational issues. However, no direction is provided on how these objectives could be used so that informed decisions can be made in the context of maximizing IS security.

As a result, the purpose of this dissertation is to develop and validate a theoretically and methodologically sound decision model that will provide a consistent and scalable means for generating informed alternatives to decision makers for the purpose of maximizing IS security in an organization. The creation of this decision model couples Dhillon and Torkzadeh's (2006) framework with Multiple Objective Decision Analysis (MODA) techniques and will be validated via an organizational case study.

The remainder of this chapter describes the nature and orientation of this research. Section 1.2 presents three definitions that are critical to this research. Section 1.3 presents the major research questions that this dissertation will address. And Section 1.4 outlines the remaining chapters of this dissertation.

1.2 Definitions

Three definitions are required to set the stage for this dissertation. The concepts defined include: *information system*, *information systems security*, and *value-focused thinking*. These concepts are embedded in the research in the subsequent chapters.

1.2.1 Information System

To adequately define the term *information system* one must first understand what the term *system* means. *Merriam Webster Online* defines the term *system* as a collection of related elements comprising a whole, where each element must be related in some way to the entire system (See also: Emery, 1981). For example, our own earth is part of a collection of planets that revolve around the sun making up what we call the solar system. To study the solar system, astronomers and physicists have discovered and defined the natural laws of gravity to explain the motion of our planets. Additionally, natural scientists have shown how our solar system is just one of millions of subsystems that make up the larger system of our galaxy and that our galaxy is just one of millions of subsystems that make up what we call the universe. In addition, natural scientists have attempted to show how the various subsystems and elements of each system in our galaxy interact with each other. For example, the motion of our own earth is influenced by the gravity of various closer planets, the sun, and our own moon where a repeating orbit around the sun is the result of these interactions. And our own solar system is known to spin around the center of our galaxy as it is impacted by the gravity of other solar systems and the gravity of the massive black hole at the center of our galaxy. The main point is that elements within a system or the subsystems within a larger system usually interact with each other creating various effects that can be studied by scientists. For this example, the end result of these various interactions is a state of relative equilibrium that results in orbital motion.

In the information systems field, the term *information system* can be viewed as a larger system that is comprised of two subsystems that include a technical and a social subsystem (Lee, 2004). Figure 1.1 illustrates the two subsystems that can be used to define an information system. As shown in Figure 1.1, the technical subsystem can be defined as a collection of software, hardware, data, and networks that interact with each other where the goal of the technical subsystem is to deliver information to the appropriate channels in the most efficient manner. The social subsystem can then be defined as the organization or various units within an organization that consists of both people and procedures that both require and create information. As shown in Figure 1.1, an information system then results from the interaction of both the social and technical subsystems.

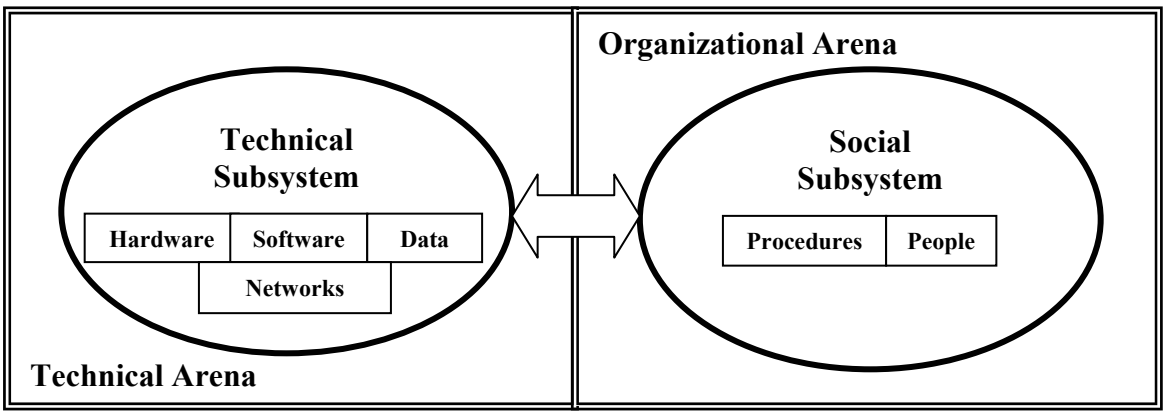

Figure 1.1: The Two Subsystems that Comprise an Information System

Lee (2004) indicates that an information system is the emergent result of the transformational interactions of the technical and social subsystems. Just like the various planets, moons, and stars in our galaxy interact with each other, so too do the two subsystems that comprise an information system. However, as Lee (2004) indicates, the effects that each of these two subsystems have on each other do not necessarily create a state of relative equilibrium like what is seen in the present orbital motion of our planets. Rather, the subsystems transform each other in an iterative and never-ending fashion. For example, once a technical subsystem is introduced to fulfill the information requirements that were created by the social subsystem, the existing technical subsystem has been changed. This technical subsystem change then triggers a change in the social subsystem which in turn triggers changes in the technical subsystem and so on. Thus, an information system is dynamic.

1.2.2 Information Systems Security

According to the United States Code (U.S. Code, 2006) the term *information systems security* means "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CIA)." *Confidentiality* refers to restricting data access to those who are interested and who should be allowed to access such data including providing a means for protecting personal privacy and proprietary information. *Integrity* refers to maintaining the values of the data stored and manipulated such that improper data modification or destruction is limited and information non-repudiation and authenticity is ensured. And *availability* refers to keeping data available

when they are needed thus ensuring timely and reliable access to the data (for a detailed discussion of CIA see: Bishop, 2002).

The definition of *information systems security* as shown in the United States Code echoes the sentiment that IS security should be approached using mostly technical constructs. However, if one conceptualizes what an *information system* is as shown in Figure 1.1, one can easily recognize that information system security must additionally contain constructs from the socio-organizational arena because the technical element has to be operated by people.

Dhillon and Backhouse (2000) share this same sentiment and note that the traditional principles of CIA apply to scenarios where information is seen as data that comes from the technical subsystem alone yet does not necessarily address the changing organizational context in which this data is interpreted and used. As a result, it can be argued that for organizations to handle security issues that emerge from the dynamic nature of information systems, an organizational subculture (Dhillon and Backhouse, 2000, pg. 127) needs to be formed that addresses the issues of responsibility, integrity, trust, and ethicality (RITE).

Responsibility refers to determining who in an organization is accountable for present and future security issues. In the context of an information system, responsibility would thus require an organization to determine who is accountable for various security operations and also policy formation that determines who will be responsible for new security threats that are not necessarily defined in the company hierarchy or some organizational chart. For example, an on-line banking Web site could be subject to new

forms of outside threats that could not necessarily be predicted because of the increasing sophistication of hackers. Thus the construct of *responsibility* addresses who in the organization is responsible for handling the dynamic nature of such threats.

Integrity (integrity of roles) refers to the issues that surround determining who in an organization should be given access to sensitive information to minimize inside threats. It is widely known that most security threats come from inside an organization. In the context of an information system such as ones that handle sensitive data (i.e., credit card information), the question then becomes who is deemed to be trusted with sensitive data so that inside threats can be minimized.

Trust refers to defining the appropriate levels of norms and patterns of behavior that all members of an organization should be trusted to implement. In the context of an information system, this concept of trust is paramount because sensitive information is often handled in the absence of close supervision. Hence levels of norms and patterns of behavior must be well-defined and explained thoroughly in company policies.

Finally, *ethicality* refers to defining ethical practices that should be followed by employees when rules defining such practices cannot be predetermined due to new and dynamic situations. In the context of an information system, the issue of ethicality is paramount because the types of data crucial to the business are constantly changing. Hence ethical policies need to be adequately communicated to the employees. To a large extent, this can be made possible by formalizing the normative structures in the organization.

Therefore, for the purposes of this dissertation, the term *information systems security* means those practices in an organization that focus on understanding, analyzing, and implementing the protection of information resources, where such protection is considered via both technical and socio-organizational issues. This definition is aligned with what Dhillon and Backhouse (2001) call the socio-organizational approach to IS security.

1.2.3 Value-Focused Thinking

Dhillon and Torkzadeh's (2006) framework of 9 fundamental and 16 means objectives for maximizing IS security provides a theoretical template for approaching IS security in a manner that transcends the technical perspective and accounts for both technical and socio-organizational issues. These objectives were derived using ideas from Keeney's (1992) value-focused thinking approach and provide the theoretical foundation for this research. Therefore, this section will briefly touch upon the notion of value-focused thinking as it relates to the decision making process. Chapter 3 will discuss value-focused thinking in more detail.

The value-focused thinking approach was derived from the field of Operations Research and offers a robust means for making decisions (Clemen, 1996). Keeney (1992, pg. 3) indicates that there are two primary methods for thinking about decisions: alternative-focused thinking (AFT) and value-focused thinking (VFT). Figure 1.2 illustrates the difference between AFT and VFT. As shown in Figure 1.2, AFT, the classical decision making technique, lists "identify alternatives" as the second step in the decision making process once the problem has been identified. Keeney (1992, pg. 6)

criticizes AFT because it tends to constrain a decision maker to a generated set of existing alternatives that often times do not reflect what is truly important for a decision. Additionally, once alternatives are determined, the decision maker is often times "anchored" (Kahneman, 2003) to this domain thus limiting the decision maker's ability to consider alternatives outside of this box (Keeney, 1992, pg. 48). In contrast to AFT, VFT first determines the values inherent to any decision context and then proposes finding creative alternatives that can adequately address these values.

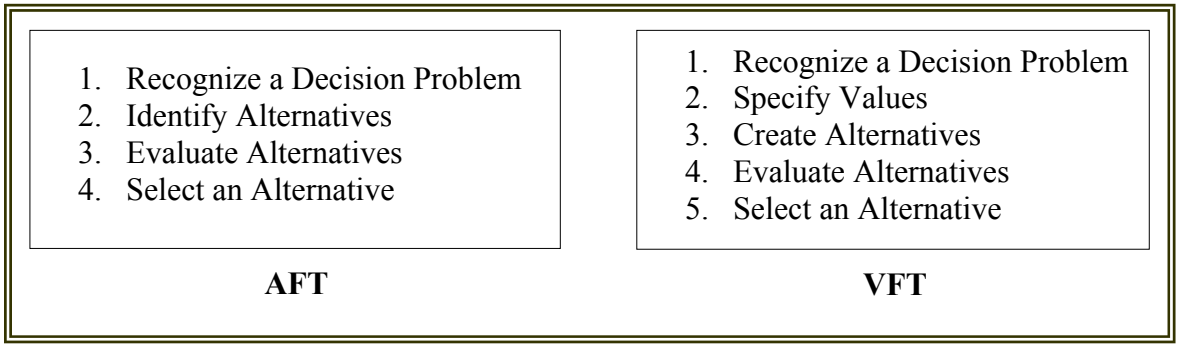

Figure 1.2: AFT versus VFT

For example, if a decision maker is tasked with determining the best way to maximize profits within an organization, a list of existing alternatives might be generated. Using the AFT approach, the decision maker would then proceed to determine which of these alternatives would be best for his or her organization and would then implement one of these alternatives without considering the underlying values inherent to this decision context. Any solution that is implemented would thus be bound to the constraints of the chosen alternative. In contrast, VFT ensures that the decision maker first figures out what is needed in the form of values and then determines the appropriate

alternatives that truly address these needs. In other words, VFT recognizes that alternatives should be the means for achieving the more fundamental and often times hidden values that lie below any decision context.

1.3 Research Problem and Objective

Dhillon and Torkzadeh's (2006) framework of 9 fundamental and 16 means objectives for maximizing IS security provides an instantiation of the first two steps of the VFT process shown in Figure 1.2. That is, they compiled a list of fundamental and means objectives that were found by directly probing the implicit values of decision makers responsible for maintaining IS security across various industry segments. These objectives provide the IS research community with a theoretical framework for addressing IS security from the socio-organizational perspective. However, without providing direction for creating, evaluating and selecting alternatives, the results of their exhaustive research efforts are limited in their practical capacity to provide decision makers with the ability to make informed decisions. Therefore, the objective of this research is to develop a methodologically sound decision model for creating, evaluating and selecting the best alternatives in the context of maximizing IS security within an organization.

1.4 Research Questions

The questions this research effort addresses include:

1. How does one develop an approach that provides a consistent means to create informed alternatives for decision makers responsible for maintaining or even maximizing IS security from the socio-organizational perspective?
2. Via the decision model created in this research, which alternatives (i.e., ideas, concepts, tasks, and solutions) should the organization studied in this research employ to maximize IS security?
3. What is the conceptual basis for creating auditing tools that can be used to maximize IS security across multiple organizational settings?

1.5 Outline of Chapters

Chapter 2 consists of a literature review and describes the current state of IS security, along with discussing in more detail, Dhillon and Torkzadeh's (2006) framework for maximizing IS security. The purpose of this initial discussion is to further demonstrate the need for approaching IS security from the socio-organizational perspective along with providing additional rationale to prove the need for further research that extends Dhillon and Torkzadeh's (2006) framework. After this need for research is developed, the various constructs (objectives) of Dhillon and Torkzadeh's (2006) framework are examined and defined more closely by analyzing various objectives against previous research. The goal of this ladder analysis is to provide a

richer understanding of these objectives as they will provide the theoretical basis of this research.

Chapter 3 identifies the theory and methodology that is used to develop the decision model created for this research. This decision model is created by coupling multi-objective decision analysis (MODA) techniques along with Dhillon and Torkzadeh's (2006) framework using a 10-step process that includes: identifying the problem (1), creating a value hierarchy (2), creating evaluation measures (3), creating value functions (4), weighting the value hierarchy (5), generating tasks (6), scoring tasks (7), conducting a deterministic analysis (8), conducting a sensitivity analysis (9), and providing recommendations (10). The goal of Chapter 3 is to develop a theoretically and methodologically sound approach for generating informed alternatives to decision makers responsible for maintaining and thus maximizing IS security across multiple organizational settings.

Chapter 4 then describes the empirical work done in this research. The major goal of Chapter 4 is to describe the organizational case study that was conducted with an organization referred to as MSI Corp. In this chapter, the organization and respondents are described and the data obtained for Steps 1–7 as shown above are presented and organized.

Chapter 5 then synthesizes the results from Chapter 4 by conducting a deterministic and sensitivity analysis. Via this analysis, Chapter 5 provides guidance to the organization in the form of informed alternatives (tasks) and recommendations for maximizing IS security.

Finally, Chapter 6 concludes the discussion generated in the previous chapters. A summary of the main contributions of this dissertation are identified along with the limitations of this research. Additionally, Chapter 6 provides directions for future research, such as creating auditing tools across various organizational segments.

Chapter 2 - Literature Review

2.1 Introduction

Because 75% of surveyed organizations have reported some type of IS security attack, there should be no surprise that several different traditional and widely accepted IS security methodologies exist (Bagchi and Udo, 2003). This chapter will compare and contrast these various methodologies to provide the justification for approaching IS security from the socio-organizational approach. Once this justification is given, this chapter then discusses Dhillon and Torkzadeh's (2006) framework of 9 fundamental and 16 means objectives used for maximizing IS security that comes from the socio-organizational arena along with providing justification for further research in this area. This chapter then defines more closely the various constructs (objectives) of Dhillon and Torkzadeh's (2006) framework by analyzing various objectives against previous research along with organizing these objectives into a more coherent form. The goal of this ladder analysis is to provide a richer understanding of these objectives as they provide the theoretical basis for this research.

2.2 Current State of IS Security

Several scholars have noted that traditional IS security methods can be classified into three distinct categories that include: checklists, risk management and formal methods (Baskerville, 1992; Backhouse and Dhillon, 1996; Siponen, 2001). Siponen

(2005) later argued that two additional IS security methods that include ISS standards and maturity criteria should be added to this list of traditional IS security methods. These five traditional methods are mostly technical in nature and are widely used by both scholars and practitioners (Siponen, 2005).

However, many researchers have noted that IS security can be more effectively handled if IS security methodologies would look beyond technical means and include various socio-organizational factors (Baskerville, 1993; Hitchings, 1996; Segev et al., 1998; Straub and Welke, 1998; Armstrong, 1999; Dhillon and Backhouse, 2001). As a result, a further IS security methodology that contains the socio-organizational perspective has begun to take hold in the IS literature stream. Siponen (2001) classifies this socio-technical research under the category of soft approaches.

Section 2.2 examines the most popular traditional methodologies of checklists, risk management and formal methods along with soft approach methodologies. The purpose of this section is to provide the justification for approaching IS security from the socio-organizational approach.

2.2.1 Checklists

Checklists created for IS security assume that various security solutions and their associated procedures can be observed and turned into a functional list that can be used by practitioners (Siponen, 2005). The underlying notion is that checklists identify what can be done rather that what needs to be done (Baskerville, 1993). Typically, checklists are created by analysts who begin by determining all known security risks and control

procedures available via a particular problem domain. A security checklist is then created that contains every conceivable control that can be implemented in a system. Practitioners who are responsible for maintaining security then analyze each control mechanism listed to determine if implementing such a control is required based on their knowledge of all known security risks for a particular problem domain.

Checklists are one of the earliest procedures used for maintaining security from a technical standpoint. Various examples of checklists include IBM's 88 point security assessment questionnaire (IBM, 1972), the SAFE checklist (Krauss, 1972), the Computer Security Handbook (Hutt *et al.*, 1988), and Moulton and Moulton's E-Com Risk Management checklist (Moulton and Moulton, 1996). These checklists offer a useful means-oriented approach to implement proper security controls, yet checklists have been criticized by both the scholar and practitioner communities. Dhillon and Backhouse (2001) criticize checklists for their lack of theoretical stability and their lack of consideration of social problems related to security. And Backhouse and Dhillon (1996, pg.4) argue, "Checklists inevitably draw concern onto the detail of procedure without addressing the key task of understanding what the substantive questions are." Practitioners have criticized checklists because the static nature of predetermined technical control can lead to security measures that do not fit the dynamic and human security requirements of an organization. For example, predetermined technical control may lead to complicated security solutions that in turn lead to poor availability of vital information (Dhillon and Torkzadeh, 2006).

2.2.2 Risk Management

The notion of risk management (RM) for IS security involves the process of measuring or assessing security risks and developing strategies to manage these risks. The methods of RM for IS security often times determine probabilities (**P**) for occurrences of particular security breaches along with the costs (**C**) associated with a given threat. Hence, the equation (**R = P * C**) is often the underlying logic of numerous IS risk management methodologies; where **R** indicates the level of risk for a particular security concern (Courtney, 1997; Baskerville, 1991).

RM for IS security is often times employed along with the use of checklists. Checklists are used to identify possible security controls, and RM techniques are used to provide a rational cost-benefit model to help eliminate unprofitable security controls (Baskerville, 1993). A few examples of RM methods include the LRAM approach (Guarro, 1987), the communication approach (Baskerville, 1991), the business focused RM method (Halliday *et al*., 1996) and the X-ifying RM method (Frisinger, 2001).

Clearly, there is a need to estimate the costs of implementing security controls and weighing these costs against the probability of a security breach. However, RM methodologies like checklists, have been criticized by several different scholars. For example, Clements (1977) regarded risk analysis techniques to be inappropriate for assessing IS security due to the high amount of error that is seen when coupling probability theory with the random nature of security breaches. Baskerville (1993) indicates that RM is seen as a product of guesswork because there are no reliable industry-wide statistics on which to base risk analysis. As a result, Baskerville (1991)

states that the real value in RM is its communication link between managers and security professionals who must make decisions concerning capital investments concerning IS security. And other scholars have criticized RM because the threats and costs associated with IS security tend to be dynamic whereas RM methods tend to be static and are based on prior knowledge (Wilcocks and Margretts, 1994; Straub and Welke, 1998; Dhillon and Torkzadeh, 2006).

2.2.3 Formal Methods

As mentioned, one disadvantage of both checklist and risk analysis techniques is that they rely on information that is already known and have limited ability to deal with the dynamic and ever-changing world of IS security. As a result, the Department of Defense (DOD) created several formal models in an attempt to dynamically manage and evaluate IS security. These models rely on high order mathematical notations and typically concentrate on the technical considerations of confidentiality, integrity and availability (CIA) for IS security. Examples of DOD formal models include the Bell LaPadula model (1973), the Denning Information Flow model, and Rushby's model.

In 1985, the National Computer Security Center (NCSC) published the Trusted Systems Evaluation Criteria (known as the "Orange Book") to provide computer vendors with an evaluation procedure to develop secure computer systems. According to Amoroso (1994), the "Orange Book" has three main goals. First, it attempts to provide a standard metric for the NCSC to compare the security of different computer systems. Second, it attempts to guide computer system vendors in the design and development of

secure systems. And third, it attempts to provide a means for specifying security requirements in government contracts.

Wing (1998) summarizes some of the major advantages of formal methods. From the designer standpoint, Wing (1998) indicates that formal methods through specification techniques help to characterize a system's behavior and properties more precisely, and through mathematical verification techniques, help to prove that a system meets its specification. However, Wing (1998) also identifies that the weakness of formal methods lies in the fact that the formal specifications of a system must always include assumptions the designer makes about the system's environment. Because environments change rapidly, often times these original assumptions that guide the formal methods no longer are correct. Additionally, clever intruders can break into a system if they can determine these assumptions. Other scholars have criticized formal methods on the basis that they rely solely on the technical considerations of CIA and do not account for socio-organizational issues (Dhillon and Backhouse, 2001).

2.2.4 Soft Approaches

As shown above, there are numerous traditional methodologies and approaches that attempt to ensure IS security. However, due to the various limitations of these approaches, along with the fact that they concentrate solely on technical matters, a number of scholars have called for a methodology that considers socio-organizational issues such as ethical practices, cultural sensitivity, responsibility, and awareness (Baskerville, 1993; Hitchings, 1996; Segev et al., 1998; Straub and Welke, 1998;

Armstrong, 1999; Dhillon and Backhouse, 2001; Dhillon and Torkzadeh, 2006). For example, Segev et al. (1998) state that the key to IS security "lies not with technology, but with the organization itself" (p. 85). Additionally, Trompeter and Eloff (2001) argue that organizational considerations of IS security should contain ethical and human components.

Siponen (2001) argues that there have been but a few isolated attempts to approach IS security using what he calls the soft approach. For example, Willcocks and Margetts (1994) assessed IS security risks and created a conceptual framework that highlights the value of historical, context-oriented analysis that served to underline the importance of the socio-organizational aspects of IS security. Straub and Welke (1998) couple interpretivist research with older forms of risk analysis. Rather than assessing security risks based on probability, Straub and Welke (1998) look for semantic matches of terms specifying degrees of risk. Strens and Dobson (1993) in their research specify security requirements using explanations in terms of roles, actions, goals and policies. And Backhouse and Dhillon (1996) in their research correlated IS security concerns with organizational communication and intentional acts of agents involved, where security is regarded as an outcome of communication breakdowns.

Hence an effort has been made to examine the socio-organizational elements of IS security. As Dhillon and Backhouse (2001, pg. 141) state, "An interpretivist understanding of information systems security concerns certainly offers advantages, furnishing a holistic view of the problem domain, especially within the scope of networked organizational forms, instead of the simplistic, one-dimensional explanation

more suitable for hierarchically structured organizations." However, soft approach methodologies have been criticized due to their lack of empirical and rigorous research along with their lack to provide a means for modeling support (Karyda et al., 2003; Dhillon and Torkzadeh, 2006).

2.3 Dhillon and Torkzadeh's (2006) Theoretical Framework

In an effort to determine measurable IS security constructs from the socio-organizational perspective, Dhillon and Torkzadeh (2006) present an array of 9 fundamental and 16 means objectives that are essential for maximizing IS security in an organization. Tables 2.1 and 2.2 illustrate these 9 fundamental and 16 means objectives respectfully, and include lower tier objectives that better define each objective. A *fundamental objective* is defined as an ultimate or an end objective that decision makers value in a specific decision context, and a *means objective* is defined as one that provides a means to achieve the ends (Keeney, 1994; Kirkwood, 1997). These objectives were created using Keeny's (1992) value-focused thinking approach via in-depth interviews with 103 managers across various organizational settings. The results were then validated for content via a panel of seven IS security experts.

Table 2.1: Fundamental Objectives for Maximizing IS Security (Dhillon and Torkzadeh, 2006)

Strategic Objective: Maximize IS Security	
First Tier (Fundamental Objective)	**Second Tier (Sub-Objective)**
F1. Enhance Management Development Practices	F1.1 Develop a management team that leads by example
	F1.2 Ensure individual comfort level of computers/software
	F1.3 Increase confidence in using computers
	F1.4 Create legitimate opportunities for financial gain
	F1.5 Provide employees with adequate IT training
	F1.6 Develop capability level of IT staff
F2. Provide Adequate Human Resource Management Practices	F2.1 Provide necessary job resources
	F2.2 Create an environment that promotes contribution
	F2.3 Encourage high levels of group morale
	F2.4 Enhance individual/group pride in the organization
	F2.5 Create an environment of employee motivation
	F2.6 Create an organizational code of ethics
F3. Develop and Sustain an Ethical Environment	F3.1 Develop an understood value system in the organization/whistle blowing
	F3.2 Develop co-worker and organizational ethical relationships
	F3.3 Instill value-based work ethics
	F3.4 Instill professional work ethics
	F3.5 Create an environment that promotes organizational loyalty
	F3.6 Stress individuals treating others as they would like to be treated
F4. Maximize Access Control	F4.1 Create user passwords
	F4.2 Provide several levels of user access
	F4.3 Ensure physical security
	F4.4 Minimize unauthorized access to information
F5. Promote Individual Work Ethic	F5.1 Maximize employee integrity in the company
	F5.2 Minimize urgency of personal gain
	F5.3 Create a desire to not jeopardize the position of the company
	F5.4 Create an environment that promotes company profitability rather than personal gain
	F5.5 Minimize temptation to use information for personal benefit
F6. Maximize Data Integrity	F6.1 Minimize unauthorized changes
	F6.2 Ensure data integrity
F7. Enhance Integrity of Business Processes	F7.1 Understand the expected use of all available information
	F7.2 Develop understanding of procedures and codes of conduct
	F7.3 Ensure that appropriate organizational controls (formal and informal) are in place
F8. Maximize Privacy	F8.1 Emphasize importance of personal privacy
	F8.2 Emphasize importance of rules against disclosure
F9. Maximize Organizational Integrity	F9.1 Create an environment of managerial support and solidarity
	F9.2 Create environment of positive management interaction
	F9.3 Create an environment that promotes respect
	F9.4 Create an environment that promotes individual reliability
	F9.5 Create environment of positive peer interaction

Table 2.2: Means Objectives for Maximizing IS Security (Dhillon and Torkzadeh, 2006)

First Tier	Second Tier
M1. Increase trust	M1.1 Display employer trust in employees
	M1.2 Develop an environment that promotes a sense of organizational responsibility
	M1.3 Maximize loyalty
M2. Provide open communication	M2.1 Minimize curiosity because of lack of information
	M2.2 Create an open-door environment within all levels of the organization
	M2.3 Stress IT department interactiveness
	M2.4 Develop open communication with IT department
	M2.5 Limit "arm's length" management
M3. Maximize awareness	M3.1 Create an environment that promotes awareness
	M3.2 Develop awareness of balance between technical and social aspects of IS security
	M3.3 Ensure explicit understanding of organizational culture by individuals
	M3.4 Educate employees to be aware about suspicious individuals and activities
M4. Optimize work allocation practices	M4.1 Distribute workload optimally
	M4.2 Monitor and adjust unoccupied time
	M4.3 Develop understanding of organizational and information use procedures
M5. Establish ownership of information	M5.1 Promote ownership in the organization
	M5.2 Emphasize importance in confidentiality
	M5.3 Emphasize the understanding of the value of information
	M5.4 Create a contract of confidentiality
M6. Clarify centralization/ decentralization issues	M6.1 Ensure a right balance between centralization and decentralization
M7. Ensure legal and procedural compliance	M7.1 Minimize the disregard for laws
	M7.2 Decrease the level of employer's tolerance for misuse of information
	M7.3 Develop understanding of legalities and regulations
	M7.4 Develop mechanisms for an information audit trail
M8. Improve authority structures	M8.1 Clarify delegation of authority
	M8.2 Minimize the need to gain excessive control
	M8.3 Link information access to an individuals' position
M9. Ensure availability of information	M9.1 Ensure adequate procedures for availability of correct information
M10. Promote responsibility and accountability	M10.1 Clarify delegation of responsibilities
	M10.2 Maximize level of commitment to organization
	M10.3 Create an environment that promotes accountability
M11. Understand work situation	M11.1 Minimize need to have leverage on others
	M11.2 Minimize desire to seek revenge on others
	M11.3 Minimize creation of disgruntled employees
M12. Maximize fulfillment of personal needs	M12.1 Appreciate personal needs for job enhancement
	M12.2 Facilitate attainment of self-actualization needs
M13. Understand individual characteristics	M13.1 Understand particular individual characteristics and demographics to subvert controls
	M13.2 Interpret individual lifestyles
M14. Enhance understanding of personal financial situation	M 14.1 Understand the needs of different level of financial status
	M14.2 Eliminate the personal benefit of sharing information with competitors
M15. Ensure censure	M15.1 Introduce a fear of being exposed or ridiculed
	M15.2 Instill a fear of consequences
	M15.3 Instill a fear of losing your job
	M15.4 Instill excommunication fear
M16. Understand personal beliefs	M16.1 Celebrate and understand the manner in which one was raised
	M16.2 Minimize the need for greed in the organization
	M16.3 Instill ethical and moral values

2.4 Analyzing the Fundamental and Means Objectives for IS Security

The objectives shown in Tables 2.1 and 2.2 emerged as a result of developing what is known as a value hierarchy (Keeney, 1992; Kirkwood, 1997). A value hierarchy is used by the decision maker as a conceptual model for generating alternatives (individual tasks for achieving value-driven objectives). It structures the organizational values beginning with the strategic objective and ending with lower level objectives used during the evaluation process. Fundamental objectives are those objectives that a decision maker actually desires to achieve in the context of a particular problem domain. And means objectives are those that promote the attainment of a fundamental objective. In other words, a means objective is used to generate the alternatives or tasks for implementing a particular fundamental objective. A hierarchy of fundamental and means objectives can then be developed as a tree with lower tier objectives serving to define in more detail what is meant by higher tier objectives. A value hierarchy ensures that the fundamental objectives are appropriately related to the strategic objective (Kirkwood, 1997) and aids an organization in identifying whether any values are missing or if any additional values are needed (Keeney, 1992).

The process for generating a value hierarchy in terms of eliciting values from respondents and how to structure these values is detailed by Keeney (1994) and was followed closely by Dhillon and Torkzadeh (2006) to generate the objectives hierarchy shown in Tables 2.1 and 2.2. In terms of identifying the values from decision makers in any given decision context, Keeney (1994) lists some techniques as shown in Table 2.3. According to Keeney (1994), if the researcher explores all of the techniques shown in

Table 2.3 with a decision maker, the output of such communication would contain a redundant list of objectives, alternatives, constraints, and evaluation measures. However, as Keeney (1994, pg. 34) states, "It is much easier to recognize redundant objectives when they are explicitly listed than it is to identify missing objectives."

Table 2.3: Techniques for Identifying Values (Keeney, 1994)

Technique	Questions
Develop a wish-list	What do you want? What do you value? What should you want?
Identify alternatives	What is a perfect alternative, a terrible alternative, some reasonable alternative? What is good or bad about each?
Consider problems and shortcomings	What is wrong or right with your organization? What needs fixing?
Predict consequences	What has occurred that was good or bad? What might occur that you care about?
Identify goals, constraints, and guidelines	What are your aspirations? What limitations are placed on you?
Consider different perspectives	What would your competitor or constituency be concerned about? At some time in the future, what would concern you?
Determine strategic objectives	What are your ultimate objectives? What are your values that are absolutely fundamental?
Determine generic objectives	What objectives do you have for your customers, your employees, your shareholders, yourself? What environmental, social, economic, or health and safety objectives are important?

After an exhaustive list of objectives, alternatives, constraints and evaluation measures is created, the next step is to isolate the objectives. Keeney (1994) defines an *objective* as a statement of something that one wants to strive towards and is characterized by three distinct features that include: a decision context, an object, and a direction of preference. For example, for the objective "maximize data integrity," the

decision context is maximizing IS security, the object is data integrity, and the direction of preference is more data integrity than less.

After a list of objectives is found, the next step is to distinguish between the fundamental and means objectives. To separate the means and fundamental objectives, Keeney (1994) recommends applying the "Why is that Important" or WITI test to each identified objective. If the answer given by the decision maker is that a particular objective is essential to a particular decision context, then that objective is a fundamental objective. If the answer given by the decision maker is that a particular objective is important because of its implications for some other objective, then that objective is a means objective.

The exact research approach that Dhillon and Torkzadeh (2006) used to generate the value hierarchy shown in Tables 2.1 and 2.2 is shown in Figure 2.1 and closely follows the approach given by Keeney (1994). Because fundamental objectives provide the ends for a particular decision context, it follows that they provide the basis for detailed qualitative and quantitative analysis for the purpose of creating and evaluating alternatives (Kirkwood, 1997). Means objectives are simply used as aid for developing creative alternatives.

As Dhillon and Torkzadeh (2006, pg. 310) state, "The value-focused objectives presented in this research offer a structured approach to promote systematic and deep thinking about objectives and hence assess the relative desirability of consequences." Additionally they state (pg. 312), "This is a significant contribution because previous research, while recognizing the importance of organizationally grounded principles, falls

short of proposing tangible measures;" yet how these objectives provide a structured approach for thinking or how these objectives could actually be measured to provide informed alternatives for decision makers responsible for maximizing IS security within an organization must be questioned.

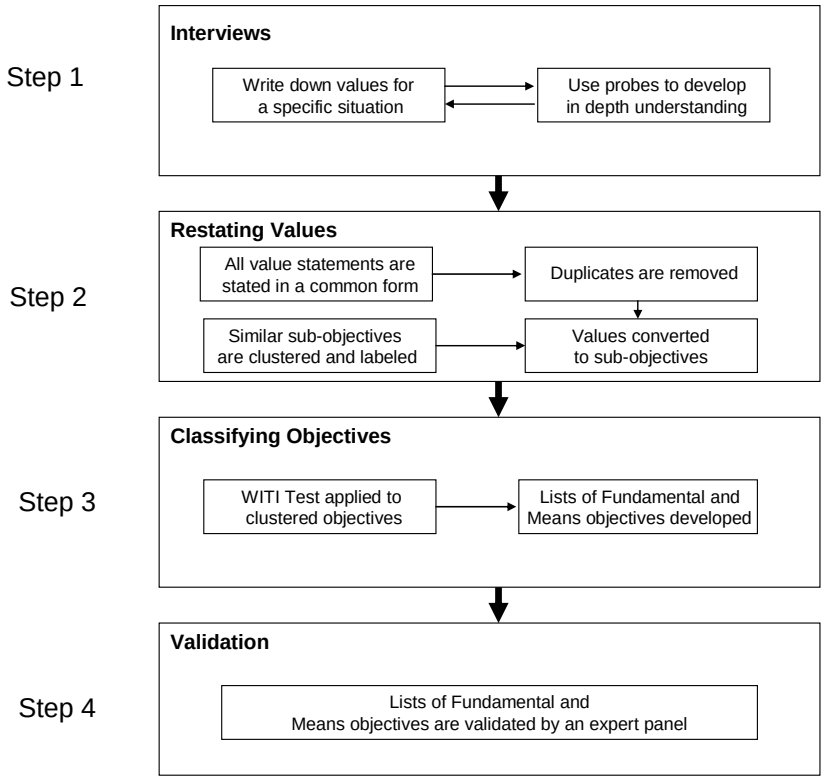

Figure 2.1: Research approach used to Generate Dhillon and Torkzadeh's (2006) Framework of 9 Fundamental and 16 Means Objectives for Maximizing IS Security

In other words, the objectives shown in Tables 2.1 and 2.2 certainly provide a theoretical template for considering IS security in a manner that accounts for both technical and organizational issues. However, without a systematic methodology or approach to provide a consistent means for assessing these objectives so that informed

decisions can be made, the decision maker is forced to rely on intuition and experience alone. Thus, the accuracy of any IS security decision made in the context of these fundamental and means objectives, as they currently stand, would be difficult to quantify. Furthermore, when decisions are made that rely on intuition and experience alone, several heuristic biases come into play that can weaken the strength of any decision (Tversky and Kahneman, 1986; Kahneman, 2003).

As a result, further research needs to be conducted that attempts to develop a methodologically sound decision model around these objectives so that informed decisions can be made for the purpose of maximizing IS security. The goal of this dissertation is to develop and validate such a decision model. However, before discussing the creation of the decision model developed in this research, various objectives are analyzed further in the context of extant literature in the remaining sections of Chapter 2.

2.4.1 Categorizing the Fundamental Objectives

As previously discussed, according to the United States Code (U.S. Code, 2006) the term *information systems security* means "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CIA)." *Confidentiality* refers to restricting data access to those who are interested and who should be allowed to access such data including providing a means for protecting personal privacy and proprietary information. *Integrity* refers to maintaining the values

of the data stored and manipulated such that improper data modification or destruction is limited and information non-repudiation and authenticity is ensured. And *availability* refers to keeping data available when they are needed thus ensuring timely and reliable access to the data. The definition of *information systems security* as shown in the United States Code echoes the sentiment that IS security should be approached using mostly technical constructs.

Upon examining the fundamental and means objectives shown in Tables 2.1 and 2.2, it becomes apparent that confidentiality, integrity, and availability of data are only a fraction of the IS security objectives identified via Dhillon and Torkzadeh's (2006) research. Dhillon and Torkzadeh (2006, pg. 309) state:

> In the past most secure system development activities and organizational security policies have been exclusively based on these three principles. Part of the problem related to our inability to manage and ensure IS security has been our over-reliance on the confidentiality, integrity and availability issues and thereby ignoring the more organizationally based measures. Even most of the risk management approaches take for granted that confidentiality, integrity and availability are the cornerstones of IS security and hence develop incomplete methodologies around these concepts. When organizations begin to over rely on risk analysis as a means to ensure IS security, they tend to ignore all the other organizationally grounded IS security vulnerabilities and problems.

When examining the 9 fundamental and 16 means objectives shown in Tables 2.1 and 2.2, it becomes apparent that both technical and social constructs emerged as being valued to IS security. In other words, Dhillon and Torkzadeh's (2006) research, which involved interviewing 103 managers about their values in relation to IS security, revealed that the management of IS security was far broader a concept than just focusing on the

technical issues of confidentiality, integrity, and availability of data. That is, the socio-organizational definition of IS security developed in Chapter 1 better defines what is shown in Tables 2.1 and 2.2 than the more technical definition seen in the U.S. code. Again, that definition of IS security is, "those practices in an organization that focus on understanding, analyzing, and implementing the protection of information resources, where such protection is considered via both technical and socio-organizational issues."

As also discussed previously, fundamental objectives provide the ends for a particular decision context. As a result, it follows that the fundamental objectives provide the focal point for further qualitative and quantitative analysis for the purpose of creating and evaluating alternatives. Figure 2.2 illustrates a conceptual hierarchy that emerges as a result of further analysis of Dhillon and Torkzadeh's (2006) research and will be used as the basis for structuring the 9 fundamental objectives for analysis throughout this dissertation. As shown in Figure 2.2, the 9 fundamental objectives can easily be broken down into two distinct categories that were developed when considering both technical and socio-organizational constructs. That is, each fundamental objective was examined and placed into either a technical or socio-organizational category. Breaking down the 9 fundamental objectives in this manner allows a more modular approach for simplifying the analysis of these objectives against each other in this section and will be beneficial for developing a weighting scheme as discussed in both Chapters 3 and 4 of this dissertation.

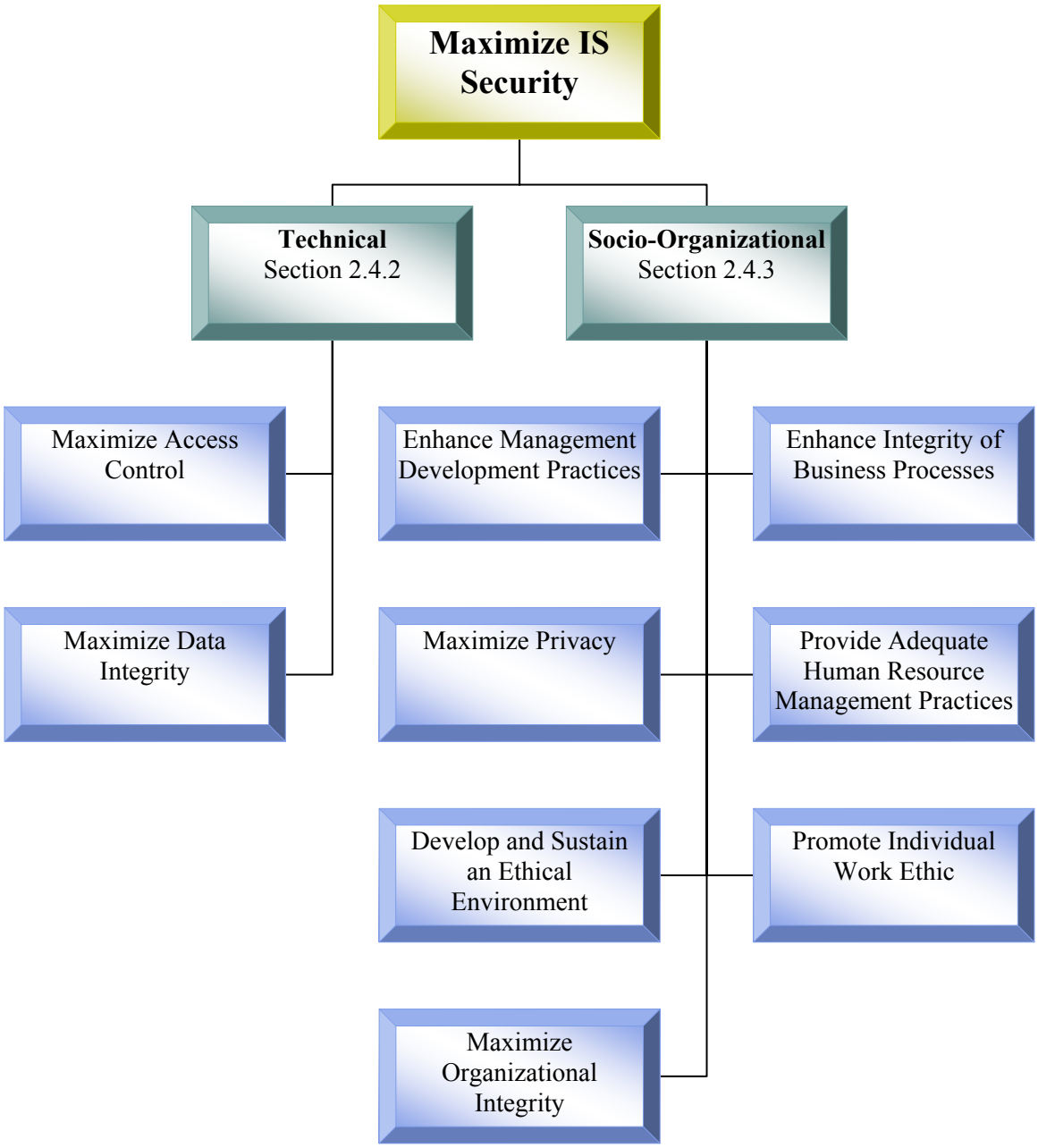

Figure 2.2: Conceptual Hierarchy of 9 Fundamental Objectives

2.4.2 Technical Constructs

As shown in Figure 2.2, the two fundamental objectives that comprise the technical component include: "Maximize Access Control" and "Maximize Data Integrity." According to the National Information Assurance Glossary (2006), *data integrity* is a condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. And *access control* means limiting access to information system resources only to authorized users, programs, processes, or other systems. In computer security, access control includes techniques for authentication, authorization, and auditing. It also includes measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems (Sandhu and Samarati, 1994).

Of the three major technical constructs of CIA, only "maximize data integrity" (F6, Table 2.1) was shown to be a fundamental objective. In their research Dhillon and Torkzadeh (2006) found that "ensure availability of information" (M9, Table 2.2) was considered to be a means objective, while confidentiality was found to be a subset of "establishing ownership of information" (M5, Table 2.2). As previously discussed, these means objectives will be used as a basis for determining creative alternatives or tasks for achieving or implementing fundamental objectives. For example, the second tier objective for "ensure availability of information" was "ensure adequate procedures for availability of correct information." Via this means objective, various alternatives or

tasks for attaining or implementing the fundamental objective of "maximize access control" may be found.

Rainer et al. (2007) provides a detailed list of important issues for the purposes of maintaining IS security. In their research, Rainer et al. (2007) provided a questionnaire to 23 business managers and 46 information security professionals that contained 142 items. Items were derived from a review of the information security literature and respondents were given the chance to add items they thought were not included in the questionnaire. Respondents were then asked to answer each item on 5-point scales ranging from "very important" to "very unimportant." Results of their research efforts indicated the top ten items for each group. Table 2.4 illustrates the results of their research efforts combined with a cross analysis with Dhillon and Torzadeh's (2006) fundamental and means objectives.

As shown in Table 2.4 most of the issues are technical in nature and can be directly linked to either a first or second tier fundamental or means objective. For example, Table 2.4 indicates that firewalls can be directly associated with the fourth fundamental objective, "maximize access control" (F4) shown in Table 2.1. Developing a sound firewall policy might then be considered a particular task for attaining the second tier objective of "minimize unauthorized access to information." Similarly, "layered defense," as shown in Table 2.4 can be directly linked to the second tier objective, "provide several levels of user access" as shown in Table 2.1.

Table 2.4: Important Technical Security Issues (Adapted from Rainer et al., 2007)

Issue	Cross Reference to Tables 2.1 and 2.2	Type
Confidentiality	M5.2→F4	Technical/Means
Integrity of Data	F6	Technical/Fundamental
Firewalls	Task→F4	Technical/Fundamental
Access Controls	F4	Technical/Fundamental
Layered Defense	F4.2→F4	Technical/Fundamental (2nd Tier)
Business Continuity Planning	**F7**	**Socio-Organizational/Fundamental**
Risk Mitigation	Task→ F4	Technical/Fundamental
Availability	M9→F4	Technical/Fundamental
Physical Security	F4.3→F4	Technical/Fundamental (2nd Tier)
Backup and Recovery	M9→F6	Technical/Means
Incident Detection	Task→F4	Technical/Fundamental
ID Theft	Task→F4	Technical/Fundamental
Virus Attacks	Task→F4	Technical/Fundamental
Defense in Depth	F4.2 → F4	Technical/Fundamental (2nd Tier)
Demilitarized Zone	Task→F4	Technical/Fundamental
Risk Management	Task→F4	Technical/Fundamental

Interestingly enough, the only socio-organizational issue that emerged at the top of the list shown in Table 2.4 was that of "business continuity planning." As shown in Table 2.4, business continuity planning is directly associated with the seventh fundamental objective shown in Table 2.1 namely, "enhance integrity of business processes." Table 2.4 will be used as a cross reference for later analysis against the findings of this dissertation when it comes to developing a comprehensive list of alternatives and tasks to attain or implement various fundamental objectives.

2.4.3 Socio-organizational Constructs

As shown in Figure 2.1, seven fundamental objectives comprise the socio-organizational layer for IS security. Because previous literature has typically focused on

the technical considerations of CIA, it should come as no surprise that with the exception of privacy, most of these socio-organizational objectives have not been widely researched in the context of IS security.

Dhillon and Backhouse (2000) note that the traditional principles of CIA apply to scenarios where information is seen as data alone yet does not necessarily address the changing organizational context in which this data is interpreted and used as information. As a result, Dhillon and Backhouse (2000) argue that for organizations to handle security issues that emerge from the dynamic nature of information systems, an organizational subculture needs to be formed that addresses the issues of responsibility, integrity, trust, and ethicality (RITE).

Responsibility refers to determining who in an organization is accountable for present and future security issues. In the context of an information system, responsibility would thus require an organization to determine who is accountable for various security operations and also policy formation that determines who will be responsible for new security threats that are not necessarily defined in the company hierarchy or some organizational chart. For example, an on-line banking Web site could be subject to new forms of outside threats that could not necessarily be predicted because of the increasing sophistication of hackers. Thus the construct of *responsibility* addresses who in the organization is responsible for handling the dynamic nature of such threats. When examining Tables 2.1 and 2.2, the *responsibility* construct was determined to be directly linked to various means objectives that included: "develop an environment that promotes a sense of organizational responsibility" (M1.2), "link information access to an

individuals' position" (M8.3) and "promote responsibility and accountability" (M10). These means objectives can then be linked to the fundamental objectives of "provide adequate human resource management practices" (F2), "develop and sustain an ethical environment" (F3), "promote individual work ethic" (F5), "maximize privacy" (F8), and "maximize organizational integrity" (F9).

Integrity (integrity of roles) refers to the issues that surround determining who in an organization should be given access to sensitive information to minimize insider threats. It is widely known that most security threats come from inside an organization (Dhillon and Moore, 2001). In the context of an information system such as ones that handle sensitive data (i.e., credit card information), the question then becomes who is deemed to be trusted with sensitive data so that inside threats can be minimized. When examining Tables 2.1 and 2.2, the *integrity* construct was determined to be represented by two fundamental objectives that included a macro and micro level objective. These two objectives were "maximize organizational integrity" (F9) and "enhance integrity of business processes" (F7).

Trust refers to defining the appropriate levels of norms and patterns of behavior that all members of an organization should be trusted to implement. In the context of an information system, this concept of trust is paramount because sensitive information is often handled in the absence of close supervision. Hence, levels of norms and patterns of behavior must be well-defined and explained thoroughly in company policies. When examining Tables 2.1 and 2.2, the *trust* construct was determined to be linked to a single means objective, namely, "increase trust" (M1). Similar to responsibility, the trust

construct can be linked to the fundamental objectives of "provide adequate human resource management practices" (F2), "develop and sustain an ethical environment" (F3), "promote individual work ethic" (F5), "maximize privacy" (F8), and "maximize organizational integrity" (F9).

Finally, *ethicality* refers to defining ethical practices that should be followed by employees when rules defining such practices cannot be predetermined due to new and dynamic situations. In the context of an information system, the issue of ethicality is paramount because the types of data crucial to the business are constantly changing. Hence ethical policies need to be adequately communicated to the employees. When examining Tables 2.1 and 2.2, the *ethicality* construct can be found in two fundamental objectives that included a macro and micro level objective. These two objectives were "develop and sustain an ethical environment" (F3) and "promote individual work ethic" (F5).

Further research that supports the socio-organizational constructs shown in Tables 2.1 and 2.2 can be found via Knapp et al. (2006). In their research, Knapp et al. (2006) conducted a survey that involved over 1000 worldwide certified information system security professionals. Their research was a combined effort of the International Information Security Certification Consortium with researchers from Auburn University. Via this survey, a ranked list of the top 25 IS security issues was developed. This list indicated that many higher ranked issues were of a managerial or socio-organizational nature. The results of their research are shown in Table 2.5 along with a cross analysis with Dhillon and Torzadeh's (2006) fundamental and means objectives.

Table 2.5: Top 25 Security Issues (Knapp et al., 2006)

Rank	Issue	Cross Reference
1	Top management support	F1.1→F1, F9.1→F9
2	User awareness training and education	M3→F8
3	Malware	Task→F4, Task→F6
4	Patch management	Task→F6
5	Vulnerability and risk management	Task→F4
6	Policy related issues (e.g., enforcement)	M7→F9
7	Organizational Culture	F2, F3, F5, F9
8	Access control	F4
9	Internal threats	Task→F9
10	Business continuity and disaster preparation	F7.3→F7
11	**Low funding and inadequate budgets**	**Cost Objective**
12	Protection of privileged information	F8
13	Network security architecture	F4.2→F4
14	Security training for IT staff	Task→F1
15	**Justifying security expenditures**	**Cost Objective**
16	Inherent insecurity of networks	F4
17	Governance	M7→(F2, F3, F5, F9)
18	Legal and regulatory issues	M7→(F2, F3, F5, F9)
19	External connectivity to organizational networks	F4
20	Lack of skilled security workforce	F1.6→F1
21	Systems development and life cycle support	Task→F7
22	Fighting spam	Task→F4
23	Firewall and IDS configurations	Task→F4
24	Wireless vulnerabilities	Task→F4
25	**Standard Issues**	**Poorly Defined**

As shown in Table 2.5, most of the top 25 issues can be linked to the various fundamental objectives shown in Table 2.1. For example, the highest ranked issue of "top management support" shown in Table 2.5, can be directly linked to the second tier objectives of "develop a management team that leads by example" (F1.1) and "create an environment of managerial support and solidarity" (F9.1) which in turn are sub-objectives of "enhance management development practices" (F1) and "maximize

organizational integrity" (F9), respectfully. For another example, the issue of patch management is not directly seen in the wording of any of the fundamental or means objectives; however, this issue could be seen as a task or alternative that could lead to the attainment or implementation of the fundamental objective of "maximize data integrity" F(6).

As also shown in Table 2.5, three issues were not accounted for in terms of being linked to the objectives shown in Tables 2.1 and 2.2. These issues include: "low funding and inadequate budgets," "justifying security expenditures," and "standard issues." The issue "standard issues" was not linked to the objectives in Tables 2.1 and 2.2 because it was not well-defined by Knapp et al. (2006). The issues of "low funding and inadequate budgets" and "justifying security expenditures" were not linked as a result of the lack of cost accounting objectives being present in Tables 2.1 and 2.2. Obviously, cost is an important objective when it comes to decision making. However, factoring in cost is outside the scope of this dissertation but should certainly be considered in future research.

2.5 Summary

This chapter examined the current state of IS security and documented some shortcomings of traditional IS security practices such as checklists, risk management, and formal methods. In short, due to the fact that these traditional techniques have been shown to concentrate solely on technical matters, a broader perspective that accounts for socio-organizational issues was found to be more appropriate when considering IS security.

This chapter then examined Dhillon and Torkzadeh's (2006) theoretical framework of 9 fundamental and 16 means objectives for maximizing IS security in an organization. These objectives were derived using a value-focused thinking approach and illustrate that both technical and socio-organizational issues are indeed valued by decision makers responsible for maintaining IS security. Dhillon and Torkzadeh's (2006) framework provides a rigorous theoretical base for considering IS security from the socio-organizational perspective; yet no current methodology exists that seeks to assess these objectives so that informed decisions can be made in the context of IS security.

This chapter then restructured Dhillon and Torkzadeh's (2006) fundamental objectives via a conceptual hierarchy (Figure 2.2) that was used to organize the analysis of these various objectives against extant literature. Table 2.6 synthesizes the results of this ladder analysis. As shown in Table 2.6, many IS security issues were found in the literature to support each of the 9 fundamental objectives. Additionally, Table 2.6 indicates that some of these security issues could be further broken down and identified as tasks for attaining or implementing various fundamental objectives.

Table 2.6: Summary of Findings from Literature Review

Fundamental Objective	Issues from Extant Literature	Tasks Found from Literature
Maximize Access Control	Confidentiality, Access Controls, Layered Defense, Availability, Physical Security, Defense in-Depth, Network Security Architecture, Inherent Insecurity of Networks, External connectivity to organizational networks	biometric scans, metal locks, hidden paths, digital signatures, encryption, social barriers, monitoring techniques, firewalls, risk mitigation, incident detection, ID theft, virus attacks, demilitarized zone, risk management, malware, vulnerability management, fighting spam, IDS configurations, wireless vulnerabilities
Maximize Data Integrity	Integrity of Data	backup and recovery, malware, patch management
Enhance Management Development Practices	Top Management Support, Lack of Skilled Security Workforce	security training
Provide Adequate Human Resource Management Practices	Governance, Legal and Regulatory Issues, Responsibility, Trust, Organizational Culture	none thus far
Develop and Sustain an Ethical Environment	Responsibility, Trust, Ethicality, Organizational Culture, Governance, Legal and Regulatory Issues	none thus far
Promote Individual Work Ethic	Ethicality, Governance, Legal and Regulatory Issues	none thus far
Enhance Integrity of Business Processes	Business Continuity Planning, Integrity of Roles	systems development and lifecycle support
Maximize Privacy	Responsibility, Trust, Protection of Privileged Information	user awareness training
Maximize Organizational Integrity	Responsibility, Integrity of Roles, Trust, Organizational Culture, Governance, Legal and Regulatory Issues	internal threat assessment

The purpose of this ladder analysis was to provide a richer understanding of these objectives as they will provide the theoretical basis for creating a decision model that will be developed in this dissertation as a means for developing various alternatives or tasks

that can be used to attain or implement these various fundamental objectives. Thus Table 2.6 will be used as a reference for checking and perhaps even identifying additional alternatives or tasks that may or may not be found later in this dissertation as a result of the organizational study that will be detailed later in this dissertation.

Chapter 3 - Theory and Research Methodology

3.1 Introduction

Dhillon and Torkzadeh's (2006) framework of 9 fundamental and 16 means objectives for maximizing IS security provides an instantiation of the first two steps of the VFT decision making process shown in Figure 1.2 in Chapter 1. These objectives illustrate that both technical and socio-organizational issues are indeed valued by decision makers responsible for maintaining IS security and provide the IS research community with a rigorous theoretical framework for addressing IS security from the socio-organizational perspective. However, without providing a direction for creating, evaluating and selecting alternatives as shown in Figure 1.2, the results of their exhaustive research efforts are limited in their practical capacity to provide decision makers with the ability to make informed decisions.

Therefore, this chapter describes the methodology used to develop a decision model for creating, evaluating and selecting the best alternatives in the context of maximizing IS security within an organization. However, before discussing this methodology, Chapter 3 first provides a theoretical description of the cognitive processes that individuals use to make decisions in an effort to identify the importance of values to the decision making process.

3.2 What are Values and How Do They Drive Decisions?

As discussed in Section 1.2.3, the notion of VFT recognizes that alternatives should be the means for achieving the more fundamental and often times hidden values that lie below any decision context (Keeney, 1992). To better understand the meaning of the above statement, this section will turn to the social psychology literature stream to provide a description of the cognitive processes associated with decision making.

According to Kahneman (2003), decision making can be studied via three cognitive processes that include: perception, intuition, and reasoning. The differences between these three cognitive processes are shown in Figure 3.1 and have been investigated by several social psychology researchers in attempts to organize the decision making process (Kahneman and Frederick, 2002; Sloman, 2002; Stanovich, 1999; Stanovich and West, 2002).

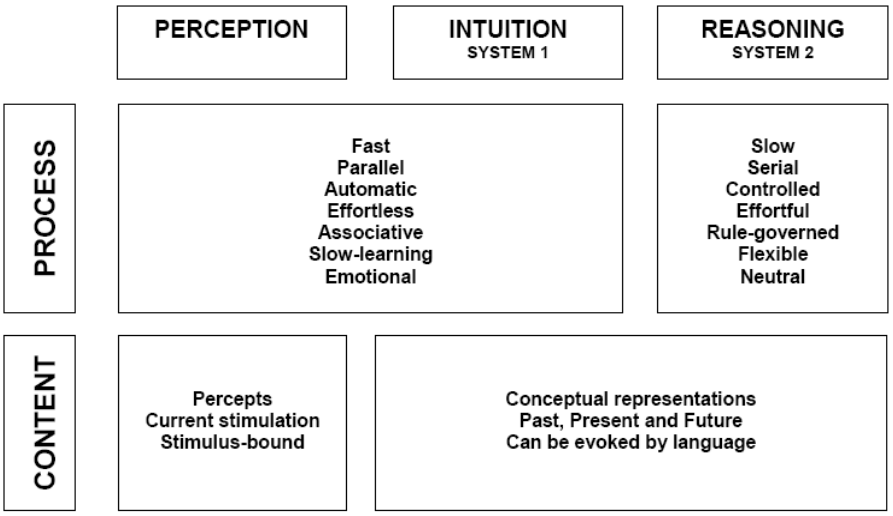

Figure 3.1: Cognitive Processes Used for Decision Making (Kahneman, 2003)

As shown in Figure 3.1, intuitive and perception-based processing is typically fast, automatic, effortless, associative, implicit, and often times emotionally charged. Kahneman (2003) indicates these processes are also governed by habit and are therefore difficult to control or modify. In contrast to intuitive and perception-based processing, the processes of reasoning are slower, require more mental effort, are more likely to be consciously monitored and deliberately controlled, and are often times governed by rules. Additionally, reasoning processes can be used to monitor or rationalize decisions that come from the intuitive and perception-based processes.

As noted by Kahneman (2003), intuitive type thinking is often times associated with poor performance as compared to reasoning type thinking. However, intuitive thinking can be powerful and accurate as an individual's experience grows. Kahneman (2003, pg. 699) states:

> High skill is acquired by prolonged practice, and the performance of skills is rapid and effortless. The proverbial master chess player who walks past a game and declares "White mates in three," without slowing is performing intuitively (Simon and Chase, 1973), as is the experienced nurse who detects subtle signs of impending heart failure (Gawande, 2002; Klein, 1998). Klein (2003, Chapter 4) has argued that skilled decision makers often do better when they trust their intuitions than when they engage in detailed analysis. In the same vein, Wilson and Schooler (1991) described an experiment in which participants who chose a poster for their own use were happier with it if their choice had been made intuitively than if it had been made analytically.

In agreeing with Kahneman, a number of other researchers have argued in the past that reasoning type thinking (i.e., deliberative, calculated decision making) is the exception and that most decisions are relatively automatic (Bargh and Chartrand, 1999; Bargh and Gollwitzer, 1994; Schneider and Shiffrin, 1977; Shiffrin and Schneider, 1977)

and are based on experience or habit (Louis and Sutton, 1991; Ronis, Yates, and Kirscht, 1989). Perhaps the reason that intuitive processes dominate decision making is that reasoning type thinking tends to delete the cognitive reservoirs of an individual. As Gabaix and Laibson (2000) indicate, "Even the simplest decisions, expressed in the conventional form of a decision tree, rapidly overwhelm human cognitive capabilities."

Regardless of whether a decision is made using reasoning or intuition, both types of thinking are similar in terms of content. That is, both intuitive and reasoning-based thinking are implicitly based on conceptual representations that are formed via the experience of the individual. These conceptual representations are what Keeney (1992) defines as values. Because of their implicit nature, Keeney (1992) argues that values are often times overlooked; yet because they provide the basis for decision making, values should in fact be what drives the creation of informed alternatives.

3.3 VFT Methodology

To generate informed alternatives from multiple objectives, a number of both qualitative and quantitative techniques can be used. One technique known as the analytic hierarchy process (AHP) has been developed for these types of problems (Saaty, 1980). In short, the AHP is a mathematical decision making technique that allows consideration of both qualitative and quantitative aspects of decisions. It reduces complex decisions to a series of pairwise (one-on-one) comparisons then synthesizes the results. However, AHP suffers from shortcomings in the area of consistency and rank reversals and can be difficult to implement with a large number of alternatives (Chambal et al., 2003).

To generate informed alternatives for the purpose of maximizing IS security, this research employs a 10-step methodology as shown in Table 3.1. This step-by-step approach combines both qualitative and quantitative techniques and was derived from the multi-objective decision analysis literature (Keeney, 1992; Keeney and Raiffa, 1993; Kirkwood, 1997; Chambal et al., 2003). Other researchers have used similar approaches for solving various problems outside the IS domain. For example, Chambal et al. (2003) used a similar methodology to provide decision makers with a decision aid for choosing a new municipal solid waste management strategy. And Merrick and Garcia (2004) used a similar approach to provide decision makers with the best alternatives for improving a particular watershed.

Table 3.1: 10-Step Research Approach

Step	Activity	VFT Process	Notes
1	Define a Strategic Objective	Recognize Decision Problem	Maximize IS Security
2	Create Amended Value Hierarchy	Specify Values	Tables 2.1 and 2.2; Organizational Study
3	Develop Evaluation Measures	Evaluate Alternatives	Organizational Study
4	Create Value Functions	Evaluate Alternatives	Organizational Study
5	Weight the Value Hierarchy	Evaluate Alternatives	Organizational Study
6	Generate Alternatives	Create Alternatives	Organizational Study
7	Score Alternatives	Evaluate Alternatives	Organizational Study
8	Deterministic Analysis	Evaluate Alternatives	Researcher
9	Sensitivity Analysis	Evaluate Alternatives	Researcher
10	Recommendations	Select an Alternative	Researcher

As shown in Table 3.1, the first two steps of this research approach have already been addressed by Dhillon and Torkzadeh (2006). Thus this dissertation extends their research to account for the remaining steps shown in Table 3.1 using an additional organizational study. The remainder of this chapter will be spent discussing the steps shown in Table 3.1 in more detail in the context of this organizational study.

3.3.1 Step 1 – Recognize a Decision Problem

The decision problem that this research addresses is maximizing IS security. For the purposes of this research, IS security is defined as those practices in an organization that focus on understanding, analyzing, and implementing the protection of information resources, where such protection is considered via both technical and socio-organizational issues. Addressing this decision problem will consist of creating a decision model. The input to this decision model will be the various value-driven objectives that will be amended via Step 2. The output of this decision model will be a ranked list of alternatives or tasks used for attaining or implementing these objectives.

3.3.2 Step 2 - Create Amended Value Hierarchy

As discussed in Chapter 2, a value hierarchy of fundamental and means objectives is used by the decision maker as a conceptual model for generating alternatives. It structures the organizational values beginning with the strategic objective and ending with lower level objectives used during the evaluation process. Fundamental objectives are those that a decision maker actually desires to achieve in the context of a particular

problem domain and for the purposes of measurement and weighting schemes, initial focus is placed on the fundamental objectives (Kirkwood, 1997). Means objectives will then be used to help in determining alternatives or tasks to attain or implement the various fundamental objectives.

As discussed, Dhillon and Torkzadeh's (2006) fundamental objectives shown in Table 2.1 were generated via in-depth interviews with 103 managers across various organizational settings. The results were then validated for content via a panel of seven IS security experts. Thus this research assumes that this framework can be deemed generalizable to any organizational setting that desires to maximize IS security. However, organizations do differ in terms of their values; therefore, these fundamental objectives are presented to the organization with the intent to verify, amend, or add objectives as deemed necessary.

Desirable properties for a value hierarchy include completeness, nonredundancy, decomposability, operability, and small size (Kirkwood, 1997). These properties are used as a starting point to evaluate the fundamental objectives via the organizational study described in Chapter 4.

The *completeness* or "collectively exhaustive" property refers to the notion that the objectives at each tier in the hierarchy must adequately cover all concerns necessary to evaluate the upper level objective and assures that alternatives are adequately evaluated and ranked accordingly. For second tier objectives, the decision makers are asked to confirm that the collection of second tier objectives are in fact complete when it comes to the first tier objectives. However, it should be noted that when analyzing the

collectively exhaustive nature of the 9 fundamental objectives as they relate to maximizing IS security, confirming that they are in fact mutually exclusive will not be a goal due to the overwhelming abundance of issues that may be involved in analyzing IS security. Thus the goal is to confirm that these 9 fundamental objectives provide a "comprehensive" list of objectives. Additionally, as previously mentioned, a cost objective is outside the scope of this research.

The *nonredundancy* or "mutually exclusive" property implies that no two objectives in the same tier of the hierarchy should have the same or similar meanings. Thus the decision makers are asked to remove any objectives that seem redundant.

The *decomposability* property refers to the notion that there must be a way to measure each objective in order to determine the overall desirability of alternatives. When investigating the objectives shown in Table 2.1, the property of *decomposability* appears to be problematic. In other words, determining measures for the second tier objectives present a challenge because the qualitative nature of these objectives do not readily allow for direct measurement. Thus creating a sound technique for measuring these objectives is investigated with care as discussed more thoroughly in Section 3.3.3.

The *operability* property refers to the notion that the objectives hierarchy should be understandable for the people who will be using it. Thus the decision makers are asked to reword various objectives so that they can be understandable to the people in their organization and to themselves.

And finally, the *small size* property refers to the notion that the hierarchy should be no bigger than necessary to minimize the duration of time spent on each of the downstream steps of the 10-step methodology shown in Table 3.1.

3.3.3 Step 3 - Develop Evaluation Measures

Once the fundamental objective hierarchy is created, evaluation measures or metrics (AKA attributes) must be developed for each of the objectives in the last tier of each branch in the hierarchy. The purpose of evaluation measures is to specify an unambiguous rating of how well an alternative or task does with respect to each objective (Kirkwood, 1997). Additionally, it should be noted that more than one measure may be needed to accurately measure a lower tier objective (Keeney, 1992).

An evaluation measure may have either a natural scale that can be measured directly or a constructed scale that is measured indirectly (Kirkwood, 1997). A natural scale that can be measured directly has a common interpretation to everyone and is thus less controversial (Keeney, 1992; Kirkwood, 1997). For example, the concentration of chlorine in a water column is typically measured using (mg/l) and can be directly measured. In contrast, a constructed scale is developed specifically for a given decision context. For example, survey questions that use a 5-point Likert rating would be considered constructed and a less direct measure of an objective (Kirkwood, 1997). As shown in Table 2.1, because there are no natural and direct means for measuring the second tier objectives, a constructed scale for each second tier objective is developed for the purposes of this research.

For the purposes of saving time within the selected organization an exhaustive list of generic questions (questionnaire) was developed (See Appendix A) to measure each of the second tier objectives shown in Table 2.1. These generic measures were then presented to the DM's where the goal was to form a more accurate set of measures that relate to the DM's specific organizational context. In addition to developing accurate, organizationally specific measures, this process also provides the DM with a first and detailed view of the fundamental objectives so that analysis for Step 2, as discussed previously, and later steps is less strenuous and more accurate.

Additionally, to create the best possible measure for each second tier objective, the finalized measures were considered from both managerial and operational perspectives of the organization. Table 3.2 illustrates an example of these measures using the first fundamental objective in Table 2.1. As shown in Table 3.2 an example of a managerial measure for objective 1.1 shown in Table 2.1 was, "You and your management team attempt to develop an environment that leads by example." The operational measure then became, "You feel that your management team attempts to develop an environment that leads by example."

Table 3.2: Example of Generic Evaluation Measures

Enhance Management Development Practices		
Sub-Objective	**Evaluation Measure (Attribute)**	
1.1 Develop a management team that leads by example	**M**	You or your management team attempt to develop an environment that leads by example.
	O	You feel that your management team attempts to develop an environment that leads by example.
1.2 Ensure individual comfort level of computers/software	**M**	You or your management team has made an effort to make your subordinates feel comfortable with using the basic features of their computers.
	M	You or someone you know has made an effort to make your subordinates feel comfortable with using the basic features of the software that they are required to use.
	MO	You feel comfortable using the basic features of your computer.
	MO	You feel comfortable using the basic features of most of the software that you are required to use
1.3 Increase confidence in using computers	**M**	You or your management team has made an effort to make your subordinates feel confident about using their computers.
	MO	You feel confident using your computer.
1.4 Create legitimate opportunities for financial gain	**MO**	You understand the importance of computer technology and how it is related to the financial well-being of your organization
1.5 Provide employees with adequate IT training	**M**	You or your management team have attempted to provide your subordinates with adequate IT training.
	O	You feel as if you have received adequate IT training.
1.6 Develop capability level of IT staff	**M**	You or your management team attempt to develop the capability level of the IT staff.
	MO	You feel as if the IT staff of your IT department is capable of handling the technology needs of your organization.

3.3.4 Step 4 - Develop Value Functions

Typically, the evaluation measures developed in the previous step are in different units and measured on different scales. Thus as Keeney (1992) notes, it is impossible to sum the individual measurements to obtain a total score. To solve this problem, value functions must be developed to transform the units of each evaluation measure into "value units" on a scale of 0 to 1 (Kirkwood, 1997).

For example, consider the question, "You and your management team attempt to develop an environment that leads by example." After discussing this measure with the DM, it could be found that a 5-point Likert scale is needed similar to the one shown in Table 3.3; yet whether or not the differences between each point on the Likert scale (ordinal data) have the same difference in value must be investigated for each measure by soliciting the DM's experience and judgment. That is, if differences in each point on the Likert scale are assumed to be the same, then the assignments of values shown in Table 3.3 could be given for each score. However, if it is determined that various measures do not have an equal change in value, then an alternative technique must be employed.

Table 3.3: Values for Evaluation Measures Assuming Equal Change in Value

Score	Meaning	Value
1	Strongly disagree	0.00
2	Disagree	0.25
3	Neither agree nor disagree	0.50
4	Agree	0.75
5	Strongly agree	1.00

For example, consider again the question, "You and your management team attempt to develop an environment that leads by example." After discussing this measure with the DM, it could be found that a bigger difference between a score of 3 and 4 and 3 and 2 exists than it does for a score of 4 and 5 and for 1 and 2. Thus the value function would look more like that shown in Figure 3.2 rather than being a straight line that would result from graphing the points shown in Table 3.3. Additionally, within a particular value model, value functions are preferred to be either all monotonically increasing or all

monotonically decreasing to establish consistency (Chambal et al., 2003). For example, a monotonically increasing value function means that the score along the x-axis increases as the value along the y-axis also increases. Subsequently, a value model having value functions that are all monotonically increasing aids those responsible for scoring the alternatives because they will know that "more is always better" when considering evaluation measures.

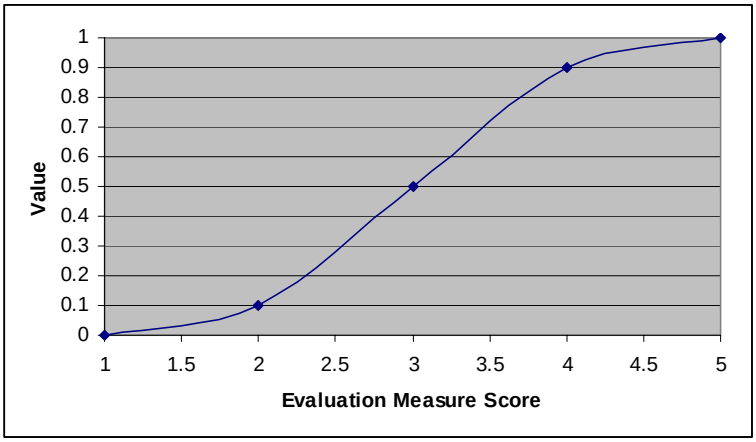

Figure 3.2: Values for Evaluation Measures with Non-Equal Changes in Value

The process for determining non-linear value functions is detailed by Kirkwood (1997, pg. 62). The process consists of first setting the lowest and highest evaluation measure scores to values of 0 and 1, respectively. The DM is then asked to consider if there is any differences in value when going from 1 to 2, 2 to 3, 3 to 4, and 4 to 5. Perhaps the DM might then indicate that the difference in going from 5 to 4 is much less than going from 4 to 3 for a particular evaluation measure and that this difference is approximately four times as great. Additionally, the DM might indicate that the same is

true on the lower end. Thus the researcher would then set the lowest increments from 1 to 2 and 4 to 5 to x and the increments from 2 to 3 and 3 to 4 to $4x$. The value of x can then be solved by recognizing that $x + 4x + 4x + x = 1$; or $x = 0.1$. The values for each evaluation measure could then be determined as shown below which would then generate the value function shown in Figure 3.2.

$$V(5) = x + 4x + 4x + x = 1.0; \; x = 0.1$$
$$\therefore \quad V(1) = 0$$
$$V(2) = x = 0.1$$
$$V(3) = x + 4x = 0.5$$
$$V(4) = x + 4x + 4x = 0.9$$

Additionally, DMs must also agree to a common definition for each point of any scales developed. In this research, as discussed in more detail in Chapter 4, it was found that the typical Likert type meanings shown in Table 3.3 are not easily interpreted. Thus alternative and more direct meanings were assigned. For example, when considering the sub-objective "develop a management team that leads by example," individual points for the value function look more like what is shown in Table 3.4. As also shown in Table 3.4, when more than one attribute is assigned to a particular sub-objective, it was found that a single-dimensional value function (SDVF) could be constructed that captures the essence of multiple evaluation measures.

Table 3.4: Defining the Points in a Value Function for Constructed Measures

1.1 Develop a management team that leads by example		
Evaluation Measures		
M	You or your management team attempt to develop an environment that leads by example.	
O	You feel that your management team attempts to develop an environment that leads by example.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this alternative is implemented to the best of its ability, it has no impact on developing a management team that leads by example. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this alternative is implemented to the best of its ability, it has a very subtle impact on developing a management team that leads by example. Impacts might be realized by either management or operational employees.	**0.3**
Mostly	If this alternative is implemented to the best of its ability, it has strong but not overwhelming impact on developing a management team that leads by example. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this alternative is implemented to the best of its ability, it will have an overwhelming impact on developing a management team that leads by example. Impacts will definitely be realized by both management and operational employees.	**1**

3.3.5 Step 5 – Weight the Value Hierarchy

The fundamental objectives hierarchy is composed of multiple objectives that should be considered when attempting to make a decision. However, each of these objectives is not necessarily equally important to a particular decision maker across various organizations. Therefore, to account for this varying degree of importance, weights must be assigned to each tier of the fundamental objective hierarchy given a particular organizational context. An important property of the hierarchy is that the local

weights for each branch and each tier, taken separately, must sum to 1.0 (Kirkwood, 1997).

Several weighting techniques exist that include: the ratio method, the swing weighting method, the trade-off method, and the pricing out method (Borcherding et al., 2003). This research will use the swing weighting technique as it has been shown to be a consistent technique that provides a fair amount of convergent validity (Borcherding et al., 2003). In using swing weights, the DM (or DMs) within a particular organization are asked to imagine the lowest tier objectives for each branch at their worst possible levels in terms of value. They are then asked to determine which objective in a group they would like to see swing to its best possible level. After choosing their most important objective within a group, they are then asked to compare their two most important objectives and state the relative importance of a full swing in each objective's attainment. After a few iterations of this technique, the researcher is then able to determine the various increments between each objective. The resulting increments are then sequentially ordered by increasing value. Each increment is then assigned a factor of importance as it relates to the smallest increment. The smallest value increment is then set so that the total of all the increments equals 1.0. The resulting increments that sum to 1.0 are then solved as a system of equations in the exact manner as shown in Step 4 above with the same number of equations and unknowns to produce the various weights. Since more than one DM is solicited for determining weights, the various weights produced are then combined and averaged to provide a final weight for each objective and attribute at each tier of the hierarchy.

To simplify the conceptual process of swing weighting the first tier objectives shown in Table 2.1, the conceptual hierarchy shown in Figure 2.2 is presented to the DMs. In other words, rather than asking the DMs to attempt to weight 9 fundamental objectives against each other, the DMs were asked to consider the technical and socio-organizational objectives by themselves and then weight the technical and socio-organizational categories independently. Figure 3.3 provides a first example of what could be found using this technique where individual weights are shown in parenthesis.

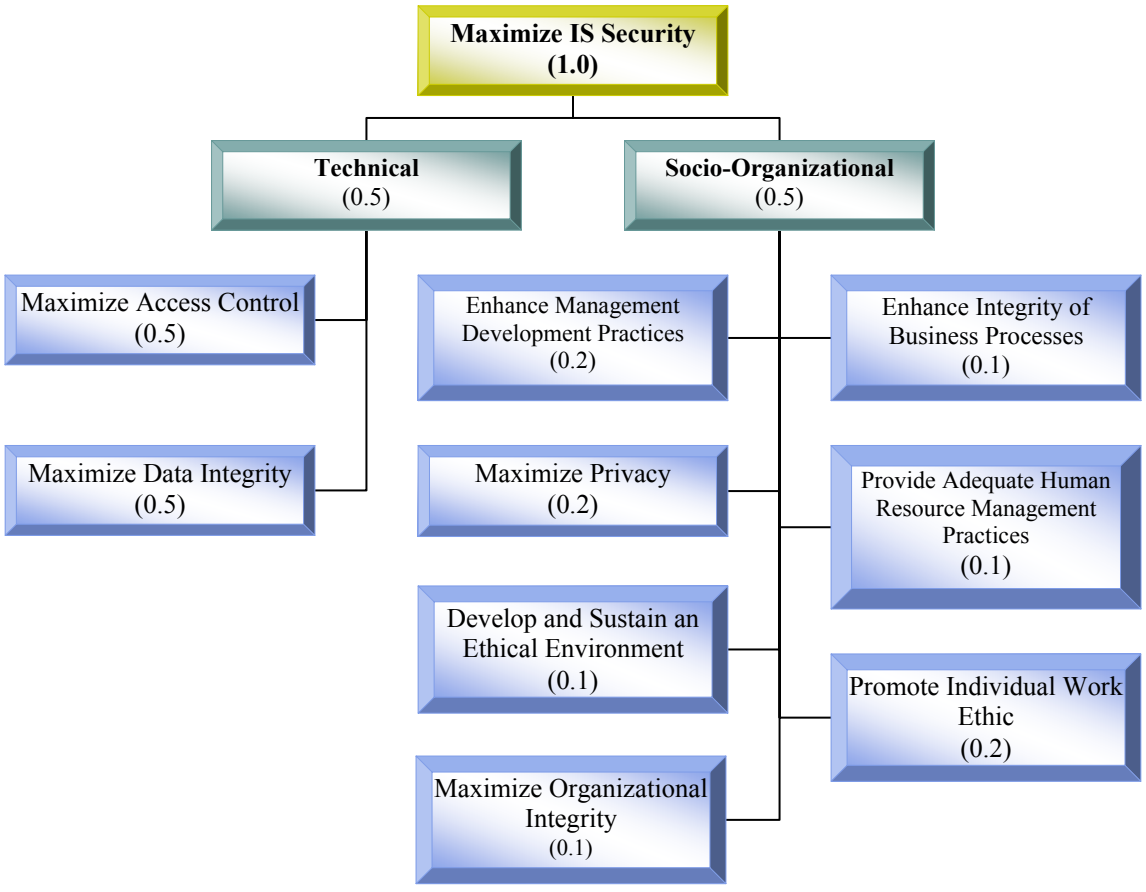

Figure 3.3: Weighting the Upper Level Objectives

3.3.6 Step 6 - Generate Alternatives

The major advantage of VFT is that it encourages the development of creative alternatives, guided by the knowledge of the organizational values (i.e., the value hierarchy shown in Table 2.1). For the purposes of this research, *alternatives* are defined as individual tasks or a collection of tasks that could be used to attain or implement the various objectives shown in Table 2.1. Depending on the situation, there are different techniques for actually generating the alternatives. To generate alternatives, the value hierarchy forces appropriate value-driven questions to be asked to accurately assess and measure the various evaluation measures for the various objectives. Via this process, alternatives are naturally created.

For this research, alternatives are generated via task generation tables. For each objective, questions are asked to determine the types of tasks required to attain or implement various objectives. Additionally, the means objectives shown in Table 2.2, provides a conceptual template for determining appropriate value-driven tasks.

3.3.7 Step 7 – Score the Alternatives

To properly use the value model, the alternatives or tasks generated in Step 6 must be scored relative to each evaluation measure. That is, each alternative received a score that ranges from the lowest to highest possible score for each evaluation measure. To determine these scores, a forum of subject matter experts (researcher, DM, outside experts) considers each alternative for a particular measure before advancing to the next measure. Ideally, the forum of subject matter experts arrives at a consensus for each

score an alternative receives. This consensus adds defensibility to the final value ranking of the alternatives because it eliminates the uncertainty factor associated with each score an alternative receives. Additionally, given the wide range of objectives as shown in Table 2.1, individual tasks only impact a small number of individual objectives. Thus the time required to accurately complete Step 7 was not too overwhelming.

3.3.8 Step 8 - Perform Deterministic Analysis

As shown in Table 2.1, over 30 second tier objectives are present. This large number of objectives ultimately led to an even larger number of tasks (69 tasks as discussed in Chapter 4). Thus the next question became, "Which of these alternatives or set of alternatives would have the most impact on maximizing IS security for a particular organization?" The goal of deterministic analysis is to allow these various tasks to be ranked in order of importance and will provide an informed and quantifiable means for justifying task selection.

To perform deterministic analysis, the data collected in the previous steps will be used to create an overall value function. There are several approaches for creating overall value functions where the additive and multiplicative value functions are the most commonly used (Chambal et al., 2003). Because the additive value function is particularly salient for prescriptive decision analysis, it will be used as a basis for this research. The additive value function assumes each single-dimensional value function contains a value of 0 for the worst level and a 1 for the best level (monotonically increasing) and that the alternatives or tasks are preferentially independent (Keeney and Raiffa, 1993). The preferential independence property essentially indicates that the choice

of a particular alternative does not impact other alternatives. With these assumptions, the additive value function is simply a weighted average of all of the various value functions and is expressed as shown in Equation 1 (Kirkwood, 1997, pg. 230):

$$(1) \quad v(x) = \sum_{i=1}^{n} w_i * v_i(x_i)$$

where, w_i = the various weights associated with the various alternative scores via the value functions $v_i(x_i)$.

Table 3.5 illustrates (using fictitious numbers for the purpose of illustration) how this deterministic analysis will be accomplished using the sixth branch ("Maximize Data Integrity") of the value hierarchy shown in Table 2.1. As mentioned in Step 5, the three weight columns are generated using the swing weighting technique via interviews with DMs. The adjusted weight (AW) column (AKA: global weight) is then calculated as W1 * W2 * W3. The measure column represents the list of evaluation measures that was created in Step 3. The alternatives column (Alt) is the actual alternatives or tasks generated via Step 6. The score column is the actual score of each alternative relative to each measure as discussed in Step 7. And finally, the value-adjusted score column (VAS) is the score adjusted via the value functions created in Step 4.

Table 3.5: Deterministic Analysis Illustration

First Tier		Second Tier		Third Tier Evaluation Measures			Alternatives		
Obj.	**Weight (W1)**	**Obj.**	**Weight (W2)**	**Measure**	**Weight (W3)**	**Adj. Weight (AW)**	**Alt**	**Score**	**Value Adj. Score (VAS)**
6	0.2	6.1	0.25	Q6.1.1	0.5	0.025	A1	Agree	0.9
							A2	Direct	1
				Q6.1.2	0.5	0.025	A2	Medium	0.5
							A3	Agree	0.9
		6.2	0.75	Q6.2.1	0.5	0.075	A3	Barely	0.1
				Q6.2.1	0.5	0.075	A2	Medium	0.5
							A4	Agree	0.75
Step 2	**Step 5**	**Step 2**	**Step 5**	**Step 3**	**Step 5**	**Step 5**	**Step 6**	**Step 7**	**Step 8**

The following calculations represent the final step in determining the best alternatives using Equation 1 and the values shown in Table 3.5. Thus, as is shown by these equations, the alternatives could be ranked in order of importance with A_2 being recommended as it would have the greatest impact on increasing the overall strategic objective of maximizing IS security.

- $V(A_1) = (0.025)(0.9) =$ **.0225**
- $V(A_2) = (0.025)(1.0)+(0.025)(0.5)+(0.075)(0.5) =$ **.0750**
- $V(A_3) = (0.025)(0.9)+(0.075)(0.1) =$ **.0300**
- $V(A_4) = (0.075)(0.75) =$ **.0563**

3.3.9 Steps 9 and 10 - Sensitivity Analysis, Final Recommendations

After the deterministic analysis is completed, the next step consisted of performing sensitivity analysis. This procedure is recommended as it examines the validity of the findings by removing the subjective nature of the weights and often times

provides the DM with valuable insight. To accomplish this analysis, the weight of each value is systematically altered and the subsequent impact on the final alternative scores and rankings are tracked. As an individual weight is changed, the other weights are adjusted to ensure that the sum of the column or section remains 1.0. The proportionality of the other weights to each other is maintained as the weight being assessed is adjusted.

Once the sensitivity analysis is complete, final recommendations are then presented to the DM. The format of the presentation depends on the insights gained during the analysis and the questions posed by the DM. It is important to communicate that this 10-step VFT process does not replace the DM; it only serves as a structured approach that provides a guide to generate informed alternatives or tasks derived from the values inherent to any decision context.

3.4 Summary

Chapter 3 discussed the theory behind the notion of value-focused thinking and described in detail the 10-step process that will be used to generate a ranked list of value-driven alternatives or tasks used to attain the various objectives shown in Table 2.1. This ranked list of value-driven tasks is used to generate valid recommendations to the organization studied in this research. Chapter 4 presents the data and results that were found as a result of implementing this 10-step VFT methodology via a single organizational study.

Chapter 4 - Data and Results

4.1 Introduction

The purpose of this chapter is to present the results of data obtained via a single organizational study. This chapter first provides a brief description of the organization chosen for obtaining data for this research followed by a brief description of the three decision makers that took part in the study. After the organization and respondents are described, this chapter then presents the data obtained for Steps 2-7 as described in Chapter 3. Chapter 5 synthesizes and discusses these results as discussed in Steps 8–10 in Chapter 3.

4.2 Organization and Respondent Profile

The organization chosen has its headquarters located in Richmond, Virginia and has been recognized as a "Most Admired Company" by *Fortune Magazine*. For anonymity purposes the organization will be referred to as MSI Corp, which represents the fact that it does business in the mortgage services industry. MSI Corp provides real estate transaction services with over 800 offices and a network of more than 10,000 active agents. It serves agent, residential, commercial, and lender customers throughout the United States, Mexico, Canada, the Caribbean, Latin America, Europe, and Asia.

MSI Corp implements various strategies for maintaining an ethical environment and the integrity of its organization. For example, a Code of Business Conduct and Ethics is presented to all new hires and every employee of MSI Corp must take and pass

a class related to it every year. Additionally, each employee of MSI Corp is required to take a computer security awareness course annually. And finally, MSI Corp ensures that all employees are made aware of its Guiding Principles as shown in Figure 4.1.

Personal Values

- **Integrity –** The personal integrity of each employee and agent representing us speaks to the integrity of our entire organization.
- **Respect for the Individual –** We respect the dignity of each individual, whether a fellow employee, customer, agent, shareholder, or member of the general public.

Drive for Excellence

- **Customer Satisfaction –** Customers are the fundamental driving force behind what we do.
- **Continuous Improvement –** There is no permanent best practice. There are always better practices. Excellence demands that we continue to find them.
- **Pursuit of Ideas –** We want ideas at all levels. Brainstorming fuels organizational energy, and high organizational energy leads to significant competitive advantages, faster delivery times, an improved scope of service, lower costs, and the ability to continuously transform.

Management Practices

- **Clear Goals and Objectives –** We set goals with a disciplined schedule. We measure results, track progress, and award achievements throughout the company. Attached to the responsibility for goal-driven results are clear and adequate authority levels, the corresponding autonomy, and appropriate measures of accountability.
- **Frequent and Open Communication –** We communicate on a regular basis. We want employees to understand company, business unit, and individual expectations and to receive timely, straightforward feedback on their performance. Feedback is a two-way street. We encourage input from every employee.
- **Employee Development –** MSI Corp is, above all else, its people. Excellence demands the ongoing training and development of each employee.
- **Teamwork –** Our responsibility is to satisfy competing demands with seamless integration of our efforts. Excellence requires cooperation.
- **Responsible Corporate Citizenship –** We seek to improve the quality of life in the communities where we live and work. We want our managers to be community-minded and we encourage our employees to be involved in their communities.

Figure 4.1: Guiding Principles of MSI Corp

4.2.1 Respondent Profile

Three auditors from MSI Corp were identified to work on this research project. For anonymity purposes these three respondents will be referred to as the Team. These three respondents hold a unique position within the company as they provide a direct link between the activities of operational employees and strategic managers. A specific duty of these auditors is to perform or direct various auditing tasks of complex application systems in production or under development for controls and security in accordance with prescribed company policies and procedures. Thus their experience and position within MSI Corp as it relates to IS security make them excellent candidates for this research. A detailed description of the specific duties for each of these three auditors can be found in Appendix D. The documentation for the various interviews with the Team is shown in Appendix B.

4.3 Value Hierarchy, Evaluation Measures, and Value Functions

An amended value hierarchy is shown in Table 4.1 and was created via three half-day sessions with the Team. The updated hierarchy shown in Table 4.1 was established by first examining Dhillon and Torkzadeh's (2006) original fundamental objectives shown in Table 2.1 along with analyzing the various second tier objectives one by one via the consideration of evaluation measures, value functions, and alternatives and the properties of being understandable to MSI Corp, being collectively exhaustive, and non-redundancy, as discussed in Chapter 3.

Table 4.1: Finalized Value Hierarchy

Overall Objective: Maximize IS Security	
First Tier	**Second Tier**
1. Maximize IT Competence	1.1 Develop a management team that leads by example
	1.2 Ensure confidence/comfort level in using computers
	1.3 Ensure an adequate understanding of the importance of computer technology and how it is related to the financial well-being of your organization
	1.4 Ensure employees have adequate IT training
	1.5 Ensure IT capability level of staff
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution
	2.2 Instill high levels of morale
	2.3 Increase/maintain pride in the organization
	2.4 Develop and maintain a motivated workforce
3. Develop and Sustain an Ethical Environment	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)
	3.2 Develop and/or make known an understood value system in the organization
	3.3 Create an environment that promotes organizational loyalty
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment
4. Maximize Access Control	4.1 Ensure personal accountability for system use
	4.2 Ensure appropriate levels of user access
	4.3 Ensure appropriate physical security
	4.4 Ensure user access is based on "need to know"
	4.5 Ensure adequate management oversight of access control issues
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company
	5.2 Create a desire to not jeopardize the reputation of the company
	5.3 Create an environment that promotes the organization's best interests rather than personal gain
	5.4 Minimize temptation to use information for personal benefit
6. Maximize Data Integrity	6.1 Ensure that inappropriate changes to data are minimized
	6.2 Ensure appropriate data integrity controls for the processing of data
	6.3 Ensure adequate management oversight of data integrity issues
7. Enhance Integrity of Business Processes	7.1 Ensure an understanding of the expected use of available information and its relation to individual business processes
	7.2 Develop procedures for managing changes to business processes
	7.3 Ensure that appropriate organizational controls are in place
8. Maximize Privacy	8.1 Emphasize importance of data privacy
	8.2 Ensure employee awareness against disclosure of sensitive data
	8.3 Ensure employees understand the repercussions of disclosing sensitive data
	8.4 Ensure that sensitive data is adequately secured
	8.5 Ensure adequate management oversight of privacy issues
9. Maximize Organizational Integrity	9.1 Create an environment that empowers employees
	9.2 Create an environment that promotes respect
	9.3 Create an environment that promotes individual reliability
	9.4 Ensure adequate management oversight of organizational integrity issues

Coming up with understandable evaluation measures, value functions, and considering alternatives subsequently forced the Team to think of the importance of each sub-objective as it relates to Information System Security. Obviously, this paid dividends for later analysis such as weighting each sub-objective relative to its peers (Section 4.4) and creating and scoring alternatives or tasks (Section 4.5) for attaining or implementing the various second tier objectives shown in Table 4.1.

The remainder of Section 4.3 describes how each fundamental objective was analyzed and discusses the evaluation measures and subsequent value function created for objective 1.1 shown in Table 4.1. Because the remaining evaluation measures and value functions for objectives 1.2-9.4 as shown in Table 4.1 were created in a similar manner to objective 1.1, detailed discussion is not warranted. However, the entire list of the evaluation measures and value functions for objectives 1.1-9.4 are shown in Appendix C.

Evaluation measures for all of the second tier objectives in Table 4.1 were created by examining the generic evaluation measures shown in Appendix A and rewording them to capture the essence of each second tier objective in a manner that the Team considered would be understandable to MSI Corp. Additionally, evaluation measures were considered from both the perspectives of management (M) and operational employees (O). The value functions were then created and worded in a manner that was consistent with the various evaluation measures so that both management and operational perspectives could be captured via one single-dimensional value function (SDVF).

4.3.1 Maximize IT Competence

As shown in Table 4.2, the original fundamental objective "Enhance Management Development Practices" was changed to "Maximize IT Competence." This change was made as a result of examining the various second tier objectives and realizing that developing IT competence within the entire organization was certainly the goal of this fundamental objective rather than just simply considering management practices. Once the Team focused on this new phrasing, the Team thought about various reasons why maximizing IT competence were important for the purpose of maximizing IS security. After some deliberation, the Team finally agreed that maximizing IT competence would serve to limit security breaches as a result of ignorance. This observation has been supported in the literature as well. For example, McGrath et al. (1995) considered deftness and comprehension as antecedents for organizational competence. And Dhillon (2008) suggests that an increased understanding of process skills helps in developing IT competence which can then lead to limiting inside threats. Of course, as IT competence is gained, unethical employees could use increased technical knowledge to their advantage in terms of getting past various security constraints. However, as shown in Table 4.1, ethical considerations are a major part of the fundamental objective hierarchy.

After the Team determined that IT competence was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable and on the property of redundancy. As shown in Table 4.2, the Team decided that the notions of comfort (F1.2) and confidence (F1.3) that were originally captured by two second tier objectives should be combined into one second tier objective

(See objective 1.2 in Table 4.2). This change was made by determining that comfort and confidence were redundant. As also shown in Table 4.2, the remainder of the original second tier objectives were either kept as is or were simply reworded to make them understandable within MSI Corp.

Table 4.2: Original and Final Second Tier Objectives for Maximize IT Competence

Original Branch	
F1. Enhance Management Development Practices	F1.1 Develop a management team that leads by example
	F1.2 Ensure individual comfort level of computers/software
	~~F1.3 Increase confidence in using computers~~
	F1.4 Create legitimate opportunities for financial gain
	F1.5 Provide employees with adequate IT training
	F1.6 Develop capability level of IT staff
Amended Branch	
1. Maximize IT Competence	1.1 Develop a management team that leads by example
	1.2 Ensure confidence/comfort level in using computers
	1.3 Ensure an adequate understanding of the importance of computer technology and how it is related to the financial well-being of your organization
	1.4 Ensure employees have adequate IT training
	1.5 Ensure IT capability level of staff

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

The five second tier objectives (objectives 1.1-1.5 in Table 4.2) were then examined in terms of being collectively exhaustive. That is, do these five objectives capture what is meant by maximizing IT competence for the purpose of maximizing IS security? As shown in Table 4.2, to maximize IT competence the Team decided that MSI Corp require that: management teams lead by example; employees of MSI Corp have a sense of confidence and feel comfortable using computer technology; employees of MSI Corp have an adequate understanding of the importance of computer technology

and how it is related to the financial well-being of the organization; managers ensure employees have adequate IT training; and managers of MSI Corp ensure the IT capability level of the staff.

Table 4.3 illustrates the evaluation measures and subsequent value function that was created for the second tier objective "develop a management team that leads by example." As shown in Table 4.3, this value function was created to capture the essence of the evaluation measures from both the managerial and operational perspectives. That is, if a given alternative or task (as discussed in Section 4.5) is thought to have no impact on both managerial or operational employees of MSI Corp, then that alternative is given a score of 0. If a given alternative or task is thought to have a limited impact on either managerial or operational employees of MSI Corp, then that alternative is given a score of 0.3. If a given alternative or task is thought to have some impact on either managerial or operational employees of MSI Corp, then that alternative is given a score of 0.5. If a given alternative or task is thought to have a strong but not overwhelming impact on both managerial or operational employees of MSI Corp, then that alternative is given a score of 0.7. And finally, if a given alternative or task is thought to have a direct impact on both managerial and operational employees of MSI Corp, then that alternative is given a score of 1.0.

After the definitions and values were created for the value function shown in Table 4.3, the Team then realized that all of the second tier objectives were related in that they all required constructed scales of similar nature. Thus it was decided that all of the value functions would be created in an analogous manner as shown in Appendix C.

Table 4.3: Evaluation Measures and Value Function for the Second Tier Objective "Develop a Management Team that Leads by Example"

1.1 Develop a management team that leads by example		
Evaluation Measures		
M	You or your management team attempt to develop an environment that leads by example for the purpose of encouraging IT competence.	
O	You feel that your management team attempts to develop an environment that leads by example for the purpose of encouraging IT competence.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts will definitely be realized by both management and operational employees.	**1**

4.3.2 Promote Employee Development and Management Practices

As shown in Table 4.4, the original fundamental objective "Provide Adequate Human Resource Management Practices" was changed to "Promote Employee

Development and Management Practices." This change was made as a result of examining the various second tier objectives and realizing that these objectives were aiming at employee development. Thus any types of activities used to promote employee development should be implemented by managers across MSI Corp rather than via Human Resources alone.

Once the Team focused on this new phrasing, the Team thought about various reasons why promoting employee development and management practices were important for the purpose of maximizing IS security. After some deliberation, the Team quickly determined that building an organization that consists of motivated and proud employees would minimize risks associated with internal security breaches. That is, a happy employee is less likely to steal from the organization. This observation has been supported in the literature as well. For example, Hitchings (1995) and Dhilon (2001) have both suggested that a positive correlation exists between disgruntled employees and security breaches.

After the Team determined that promoting employee development and management practices was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable and on the property of redundancy. As shown in Table 4.4, the Team decided that redundant objectives were not present. However, many of the second tier objectives were reworded to make them understandable within MSI Corp.

Table 4.4: Original and Final Second Tier Objectives for Promote Employee Development and Management Practices

Original Branch	
F2. Provide Adequate Human Resource Management Practices	*F2.1 Provide necessary job resources*
	F2.2 Create an environment that promotes contribution
	F2.3 Encourage high levels of group morale
	F2.4 Enhance individual/group pride in the organization
	F2.5 Create an environment of employee motivation
	F2.6 Create an organizational code of ethics
Amended Branch	
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution
	2.2 Instill high levels of morale
	2.3 Increase/maintain pride in the organization
	2.4 Develop and maintain a motivated workforce

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

Additionally, two original second tier objectives were removed because the Team determined that they were in fact alternatives or tasks rather than objectives. These two objectives were "provide necessary job resources" (F2.1) and "create an organizational code of ethics" (F2.6). The original second tier objective "provide necessary job resources" was determined to be a task that could help to implement or attain all of the objectives (objectives 2.1-2.4) in this branch. And the original second tier objective "create an organizational code of ethics" was considered a task that could help to implement or attain the second tier objectives for "Develop and Sustain an Ethical Environment" (objective 3).

The four remaining second tier objectives (objectives 2.1–2.4) were then examined in terms of being collectively exhaustive. That is, do these four objectives capture what is meant by promoting employee development and management practices

for the purpose of maximizing IS security? As shown in Table 4.4, to promote employee development and management practices for the purpose of maximizing IS security the Team decided that MSI Corp require that: management teams of MSI Corp create an environment that promotes contribution; management teams instill high levels of morale to employees of MSI Corp; management teams increase/maintain pride amongst employees of MSI Corp; and managers develop and maintain a motivated workforce.

4.3.3 Develop and Sustain an Ethical Environment

As shown in Table 4.5, the fundamental objective "Develop and Sustain an Ethical Environment" was kept in its original form. The Team then thought about various reasons why developing and sustaining an ethical environment was important for maximizing IS security and how it was different from other objectives such as "Promoting Individual Work Ethic" (objective 5). After some deliberation, the Team determined that developing and sustaining an ethical environment was obviously important due to the fact that the work environment has a major impact on the actions of individuals in any organization in terms of added security (James, 1996). Thus this objective was considered a macro level objective whereas the fundamental objective "Promoting Individual Work Ethic" was considered a micro level objective. That is, both objectives work together in a symbiotic manner from environment to the individual back to the environment with the goal being to build strong ethical foundations in the organization.

After the Team determined that developing and sustaining an ethical environment was important for maximizing IS security, the various second tier objectives were

examined in terms of wording that was understandable and on the property of redundancy. As shown in Table 4.5, the Team decided that redundant objectives were not present. However, most of the second tier objectives were reworded to make them understandable within MSI Corp.

Additionally, four original second tier objectives were removed because the Team determined that they were in fact alternatives or tasks that could be used as a means for attaining the various second tier objectives of this branch rather than being second tier objectives themselves. These four objectives were "discourage unethical relationships" (F3.2), "instill value-based work ethics" (F3.3), "instill professional-based work ethics" (F3.4), and "stress individuals treating others as they would like to be treated" (F3.6). For example, it could certainly be argued that "stressing individuals in MSI Corp treating others as they would like to be treated" would be one task of the actual second tier objective "develop and/or make known an understood value system" (objective 3.2).

The two remaining second tier objectives shown in Table 4.5 (objectives 3.1 and 3.3) were then examined in terms of being collectively exhaustive. That is, do these two objectives capture what is meant by developing and sustaining an ethical environment for the purpose of maximizing IS security? As shown in Table 4.5, to develop and sustain an ethical environment for the purpose of maximizing IS security the Team decided that MSI Corp require that: management teams of MSI Corp create an environment that makes it acceptable to report unethical behavior (whistle blowing); management teams develop and/or make known an understood value system in the organization to employees of MSI Corp; management teams create an environment that promotes organizational

loyalty amongst employees of MSI Corp; and upper level or strategic managers ensure adequate management oversight of developing and sustaining an ethical environment for the purpose of maximizing IS security.

Table 4.5: Original and Final Second Tier Objectives for Develop and Sustain an Ethical Environment

Original Branch	
F3. Develop and Sustain an Ethical Environment	F3.1 Develop an understood value system in the organization/ whistle blowing
	F3.2 Develop co-worker and organizational ethical relationships
	F3.3 Instill value-based work ethics
	F3.4 Instill professional work ethics
	F3.5 Create an environment that promotes organizational loyalty
	F3.6 Stress individuals treating others as they would like to be treated
Amended Branch	
3. Develop and Sustain an Ethical Environment	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)
	3.2 Develop and/or make known an understood value system in the organization
	3.3 Create an environment that promotes organizational loyalty
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

As shown in Table 4.5, two of these final second tier objectives (objectives 3.2 and 3.4) were added for the purpose of being collectively exhaustive. Objective 3.2 was added because it captures the essence of the environmental aspect of this fundamental objective. That is, developing and/or making known an understood value system in the organization to employees of MSI Corp must be considered if an organization desires to

create an environment that will in fact impact various individuals of that organization. And objective 3.4, "ensure adequate management oversight of developing and sustaining an ethical environment" was added because it was thought that upper level managers needed to be involved in keeping a keen eye on developing and sustaining this fundamental objective. That is, lower level managers at MSI Corp might be less inclined to give much attention to this fundamental objective without the strong supervision of upper level managers.

4.3.4 Maximize Access Control

As shown in Table 4.6, the fundamental objective "Maximize Access Control" was kept in its original form. Additionally, because of the technical and widely accepted nature of this fundamental objective, as discussed in Chapter 2, the Team had no problem with accepting it as being extremely important for maximizing IS security. Issues such as accountability, user access, and physical security were at the heart of the discussions with the Team.

After the Team discussed the various reasons why access control was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable to MSI Corp and on the property of redundancy. As shown in Table 4.6, the Team decided that redundant objectives were not present. However, most of the second tier objectives were reworded to make them understandable within MSI Corp and so that these objectives could be implemented and monitored via both technical and non-technical managers. For example, to "ensure appropriate levels of

user access" (objective 4.2) requires a certain amount of technical expertise or knowledge from both the IT department to implement and from various managers throughout the organization to monitor.

Table 4.6: Original and Final Second Tier Objectives for Maximize Access Control

Original Branch	
F4. Maximize Access Control	*F4.1 Create user passwords*
	F4.2 Provide several levels of user access
	F4.3 Ensure physical security
	F4.4 Minimize unauthorized access to information
Amended Branch	
4. Maximize Access Control	**4.1 Ensure personal accountability for system use**
	4.2 Ensure appropriate levels of user access
	4.3 Ensure appropriate physical security
	4.4 Ensure user access is based on "need to know"
	4.5 Ensure adequate management oversight of access control issues

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

Additionally, one original second tier objective, "create user passwords" (F4.1), was removed because the Team determined that it was an alternative or task that could be used as a means for attaining the second tier objectives. For example, creating a well-designed password policy would certainly provide a means for attaining the second tier objective of "ensure user access is based on 'need to know'" (objective 4.4).

The three remaining second tier objectives (objectives F4.2–F4.4) were then examined in terms of being collectively exhaustive. That is, do these three second tier objectives capture what is meant by maximizing access control for the purpose of maximizing IS security? As shown in Table 4.6, to maximize access control for the

purpose of maximizing IS security the Team decided that MSI Corp require that management teams of MSI Corp ensure: personal accountability for system use; appropriate levels of user access; appropriate physical security; user access is based on "need to know;" and upper level or strategic managers ensure adequate management oversight of access control issues for the purpose of maximizing IS security.

Three of these final second tier objectives shown in Table 4.6 (objectives 4.1, 4.4, and 4.5) were added for the purpose of being collectively exhaustive. Objectives 4.1 and 4.4 were added because accountability and providing information on a "need to know" basis were already established objectives within MSI Corp. And objective 4.5, "ensure adequate management oversight of access control issues," was added because again it was thought that upper level managers needed to be involved in keeping a keen eye on access control issues. That is, because access control was considered a very important objective, strong supervision of this objective via upper level managers was added to this branch. Providing added supervision for access control issues is supported by Strens and Dobson (1993) as they advocate for creating models of responsibility structures for ensuring security.

4.3.5 Promote Individual Work Ethic

As shown in Table 4.7, the fundamental objective "Promote Individual Work Ethic" was kept in its original form. The Team then thought about various reasons why promoting individual work ethic was important for maximizing IS security and how it was different from "Develop and Sustain an Ethical Environment" (objective 3). As mentioned in Section 4.3.3, objective 5 is concerned with ethical issues at the micro or

individual level of the organization. Additionally, the Team recognized that this micro level objective not only collaborates in a symbiotic manner with objective 3 (macro level ethical issue) but also collaborates with objective 9, "Maximize Organizational Integrity" (macro level integrity issue). Thus employee integrity (micro level integrity issue) and minimizing personal gain (micro level ethical issue) were main issues of consideration.

Table 4.7: Original and Final Second Tier Objectives for Promote Individual Work Ethic

Original Branch	
F5. Promote Individual Work Ethic	F5.1 Maximize employee integrity in the company
	~~F5.2 Minimize urgency of personal gain~~
	F5.3 Create a desire to not jeopardize the position of the company
	F5.4 Create an environment that promotes company profitability rather than personal gain
	F5.5 Minimize temptation to use information for personal benefit
Amended Branch	
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company
	5.2 Create a desire to not jeopardize the reputation of the company
	5.3 Create an environment that promotes the organization's best interests rather than personal gain
	5.4 Minimize temptation to use information for personal benefit

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

After the Team determined that promoting individual work ethic was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable and on the property of redundancy. As shown in Table 4.7, the Team decided that the original second tier objective "minimize urgency of personal gain" was somewhat redundant in that it was addressed as an access control objective. Thus it was removed from this branch. Additionally, as shown in Table 4.7,

one of the second tier objectives (F5.4) was reworded to make it more understandable within MSI Corp.

The four final second tier objectives shown in Table 4.7 (objectives 5.1–5.4) were then examined in terms of being collectively exhaustive. That is, do these four objectives capture what is meant by promoting individual work ethic for the purpose of maximizing IS security? As shown in Table 4.7, to promote individual work ethic for the purpose of maximizing IS security the Team decided that MSI Corp require that management teams: maximize employee integrity in the company; create a desire for employees to not jeopardize the reputation of the company; create an environment that promotes the organization's best interests rather than the personal gain of individual employees; and minimize the temptation for employees of MSI Corp to use information for personal benefit.

4.3.6 Maximize Data Integrity

As shown in Table 4.8, the fundamental objective "Maximize Data Integrity" was kept in its original form. Similar to maximizing access control, the Team had no problem with accepting this widely known technical objective as being extremely important for maximizing IS security. That is, if the integrity of data within an organization is compromised, then any information used to make decisions about daily operations or strategic advancement is severely limited. This observation has been supported in the literature as well. For example, both Dunn (1990) and Boockholdt (1987) have explicitly argued that data integrity leads to enhanced executive decisions. Thus data must be

unchanged from its source and actions must be taken so that data is not accidentally or maliciously modified, altered, or destroyed.

Table 4.8: Original and Final Second Tier Objectives for Maximize Data Integrity

Original Branch	
F6. Maximize Data Integrity	F6.1 Minimize unauthorized changes
	F6.2 Ensure data integrity
Amended Branch	
6. Maximize Data Integrity	6.1 Ensure that inappropriate changes to data are minimized
	6.2 Ensure appropriate data integrity controls for the processing of data
	6.3 Ensure adequate management oversight of data integrity issues

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

After the Team discussed the obvious reasons why data integrity was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable to MSI Corp and on the property of redundancy. As shown in Table 4.8, the Team decided that redundant objectives were not present. However, the two original objectives were reworded to make them understandable within MSI Corp and so that these objectives could be implemented and monitored via both technical and non-technical managers. For example, the original objective "ensure data integrity" (objective F6.2) was thought to be too broad. Thus it was changed to "ensure appropriate data integrity controls for the processing of data" (objective 6.2). Via this new wording, it becomes apparent that objective 6.2 as shown in Table 4.8 requires a certain amount of technical expertise or knowledge from both the IT department to implement and from various managers throughout the organization to monitor (Maletic and Marcus, 2000).

The two remaining second tier objectives (objectives 6.1 and 6.2) were then examined in terms of being collectively exhaustive. That is, do these three second tier objectives capture what is meant by maximizing data integrity for the purpose of maximizing IS security? As shown in Table 4.8, to maximize data integrity for the purpose of maximizing IS security the Team decided that MSI Corp require that management teams of MSI Corp ensure that: inappropriate changes to data are minimized; appropriate data integrity controls for the processing of data; appropriate physical security; and upper level or strategic managers of MSI Corp ensure adequate management oversight of data integrity issues for the purpose of maximizing IS security.

As shown in Table 4.8, the second tier objective "ensure adequate management oversight of data integrity issues" (objective 6.3) was added for the purpose of being collectively exhaustive. Similar to access control, objective 6.3 was added because again it was thought that upper level managers needed to be involved in keeping a keen eye on data integrity issues. That is, because data integrity was considered a very important objective, strong supervision of this objective via upper level managers was added to this branch.

4.3.7 Enhance Integrity of Business Processes

As shown in Table 4.9, the fundamental objective "Enhance Integrity of Business Processes" was kept in its original form. The Team then thought about various reasons why enhancing the integrity of business processes was important for maximizing IS security. After a brief deliberation, it was quickly determined that if data integrity is an important issue then enhancing the integrity of business processes should be a very

important issue as well. This same sentiment is expressed by Herrmann and Pernul (1999). That is, if employees are more aware of how information pertains to various business processes of an organization, these same employees will be more inclined to protect this information.

Table 4.9: Original and Final Second Tier Objectives for Enhance Integrity of Business Processes

Original Branch	
F7. Enhance Integrity of Business Processes	F7.1 Understand the expected use of all available information
	F7.2 Develop understanding of procedures and codes of conduct
	F7.3 Ensure that appropriate organizational controls (formal and informal) are in place
Amended Branch	
7. Enhance Integrity of Business Processes	7.1 Ensure an understanding of the expected use of available information and its relation to individual business processes
	7.2 Develop procedures for managing changes to business processes
	7.3 Ensure that appropriate organizational controls are in place

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

After the Team determined that enhancing the integrity of business processes was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable and on the property of redundancy. As shown in Table 4.9, the Team decided that redundant objectives were not present. Additionally, as shown in Table 4.9, minimal changes were made in terms of rewording these second tier objectives to make them more understandable within MSI Corp.

The three final second tier objectives shown in Table 4.9 (objectives 7.1–7.3) were then examined in terms of being collectively exhaustive. That is, do these three objectives capture what is meant by enhancing the integrity of business processes for the

purpose of maximizing IS security? As shown in Table 4.9, to enhance the integrity of business processes for the purpose of maximizing IS security the Team decided that MSI Corp require that management teams: ensure an understanding to MSI Corp employees of the expected use of available information and its relation to individual business processes; develop procedures for managing changes to business processes; and ensure that appropriate organizational controls are in place.

4.3.7 Maximize Privacy

As shown in Table 4.10, the fundamental objective "Maximize Privacy" was kept in its original form. The Team then thought about various reasons why maximizing privacy was important for maximizing IS security. After some deliberation, the Team determined that employees of MSI Corp would be less inclined to accidentally or even maliciously expose sensitive data if they were more aware of how sensitive various data are and of the various repercussions that could result.

Table 4.10: Original and Final Second Tier Objectives for Maximize Privacy

Original Branch	
F8. Maximize Privacy	F8.1 Emphasize importance of personal privacy
	F8.2 Emphasize importance of rules against disclosure
Amended Branch	
8. Maximize Privacy	8.1 Emphasize importance of data privacy
	8.2 Ensure employee awareness against disclosure of sensitive data
	8.3 Ensure employees understand the repercussions of disclosing sensitive data
	8.4 Ensure that sensitive data is adequately secured
	8.5 Ensure adequate management oversight of privacy issues

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

After the Team determined that maximizing data privacy was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable and on the property of redundancy. As shown in Table 4.10, the Team decided that redundant objectives were not present. Additionally, as shown in Table 4.10, minimal changes were made in terms of rewording the two second tier objectives F8.1 and F8.2.

The two original second tier objectives shown in Table 4.10 (objectives F8.1 and F8.2) were then examined in terms of being collectively exhaustive. That is, do these two objectives capture what is meant by maximizing data privacy for the purpose of maximizing IS security? As shown in Table 4.10, three additional objectives were added to the list. Thus to maximize data privacy for the purpose of maximizing IS security, the Team decided that MSI Corp require that management teams: emphasize importance of data privacy; ensure employee awareness against disclosure of sensitive data; ensure employees understand the repercussions of disclosing sensitive data; ensure that sensitive data is adequately secured; and upper level or strategic managers of MSI Corp ensure adequate management oversight of privacy issues.

4.3.9 Maximize Organizational Integrity

As shown in Table 4.11, the fundamental objective "Maximize Organizational Integrity" was kept in its original form. The Team then thought about various reasons why maximizing organizational integrity was important for maximizing IS security. After much deliberation, the Team finally defined integrity as being able to count on

someone to do what is expected. This definition provided a contrast against ethics. In other words, you can have integrity but still be unethical (see Curtin, 2000). Thus because ethics was determined important, then this fundamental objective was determined to be important for maximizing IS security and was considered non-redundant with ethical issues.

After the Team determined that maximizing organizational integrity was important for maximizing IS security, the various second tier objectives were examined in terms of wording that was understandable and on the property of redundancy. As shown in Table 4.11, the Team decided that the original second tier objective "create an environment of positive management interaction" (F9.2) was redundant with "create an environment of managerial support and solidarity" (F9.1). Additionally, the team determined that "create an environment of positive peer interaction" (F9.5) was redundant with "create an environment that promotes respect" (F9.3). As a result, objectives F9.2 and F9.5 were removed. Additionally, as shown in Table 4.11, the remaining second tier objectives were minimally reworded to make them more understandable within MSI Corp.

Additionally, as shown in Table 4.11, one original second tier objective, "create an environment of managerial support and solidarity," was removed because the Team determined that it was an alternative or task that could be used as a means for attaining the second tier objectives. For example, creating an environment of managerial support and solidarity would certainly be a means for attaining the second tier objective of "create an environment that promotes respect" (objective 9.2).

Table 4.11: Original and Final Second Tier Objectives for Maximize Organizational Integrity

Original Branch	
F9. Maximize Organizational Integrity	*F9.1 Create an environment of managerial support and solidarity*
	~~F9.2 Create environment of positive management interaction~~
	F9.3 Create an environment that promotes respect
	F9.4 Create an environment that promotes individual reliability
	~~F9.5 Create environment of positive peer interaction~~
Amended Branch	
9. Maximize Organizational Integrity	**9.1 Create an environment that empowers employees**
	9.2 Create an environment that promotes respect
	9.3 Create an environment that promotes individual reliability
	9.4 Ensure adequate management oversight of organizational integrity issues

- *Italicized* objectives were removed as a result of being deemed tasks
- ~~Crossed out~~ objectives were removed as a result of being redundant
- **Bolded** objectives were added to ensure the property of being collectively exhaustive

The two remaining second tier objectives shown in Table 4.10 (F9.3 and F9.4) were then examined in terms of being collectively exhaustive. That is, do these two objectives capture what is meant by maximizing organizational integrity for the purpose of maximizing IS security? As shown in Table 4.10, to promote individual work ethic for the purpose of maximizing IS security the Team decided that MSI Corp require that management teams: create an environment that empowers employees; create an environment that promotes respect; create an environment that promotes individual reliability; and upper level or strategic managers of MSI Corp ensure adequate management oversight of organizational integrity issues.

4.4 Weights

As shown in Table 4.1, the fundamental objectives hierarchy is composed of multiple objectives that should be considered when attempting to make decisions about what types of alternatives or tasks should be implemented for the purpose of maximizing IS security. However, each of these objectives is not necessarily equally important to a particular decision maker across various organizations. Therefore, to account for this varying degree of importance, weights must be assigned to each tier of the fundamental objective hierarchy given a particular organizational context. An important property of the hierarchy is that the local weights for each branch and each tier, taken separately, and the finalized global weights across all branches must sum to 1.0.

To determine the weights of the various objectives shown in Table 4.1, the swing weighting technique was used for both tiers of objectives starting at the lowest tier. In using swing weights, individuals from the Team were first asked to imagine the lowest tier objectives for each branch at their worst possible levels in terms of value. For example, when considering "Maximize Data Integrity," the respondent was asked to imagine scenarios such as shown in Table 4.12.

Table 4.12: Example Questions Used to Imagine Objectives at their Worst Possible Level for Swing Weighting

Second Tier Objective	Worst Possible Level
6.1 Ensure that inappropriate changes to data are minimized	Your organization does not care about whether or not data is changed inappropriately.
6.2 Ensure appropriate data integrity controls for the processing of data	Your organization does not ensure appropriate controls for data integrity.
6.3 Ensure adequate management oversight of data integrity issues	There is no management oversight of data integrity issues.

Respondents were then asked to consider which of these objectives they would like to see swing to its best possible level. After choosing their most important objective within a group, respondents were then asked to compare their two most important objectives and state the relative importance of a full swing in each objective's attainment. After a few iterations of this technique, various increments between each objective were determined. The lowest ranked objective was then assigned a value of X and the remaining objectives were assigned multiples of X. For example, if OBJ6.1 and OBJ6.2 shown in Table 4.3 were considered to be the least important objectives and OBJ6.3 was considered to be three times as important, then OBJ6.1 and OBJ6.3 were assigned values of X and OBJ6.3 would have been assigned a value of 3X. After these values of X were assigned, weights were easily determined by recognizing that the sum of the weights in an individual branch must be equal to 1. For the above example, weights would be determined via the following equations

- X + X + 3X = 1
  - X = 1/5 = 0.200
    - **OBJ6.1W** = 0.200
    - **OBJ6.2W** = 0.200
    - **OBJ6.3W** = 3 * 0.200 = 0.600

Table 4.13 illustrates the average local weights for each of the second tier objectives. As shown in Table 4.13, two individuals from the Team were taken through this process. Thus the final local weight was determined by averaging across the results of both respondents.

Table 4.13: Local Weights for the Second Tier Objectives

Objective		Auditor 1		Auditor 2		Average Local Weight	Branch Sum
First Tier	Second Tier	X Value	Weight	X Value	Weight		
1. Maximize IT Competence	1.1	X	0.143	X	0.138	0.14	1.0
	1.2	X	0.143	X	0.138	0.14	
	1.3	X	0.143	1.5X	0.207	0.175	
	1.4	1.5X	0.214	1.75X	0.241	0.228	
	1.5	2.5X	0.357	2X	0.276	0.317	
2. Promote Employee Development/Management Practices	2.1	X	0.250	X	0.250	0.25	1.0
	2.2	X	0.250	X	0.250	0.25	
	2.3	X	0.250	X	0.250	0.25	
	2.4	X	0.250	X	0.250	0.25	
3. Develop and Sustain an Ethical Environment	3.1	X	0.133	2.5X	0.278	0.206	1.0
	3.2	3X	0.400	2.5X	0.278	0.339	
	3.3	1.5X	0.200	X	0.111	0.156	
	3.4	2X	0.267	3X	0.333	0.3	
4. Maximize Access Control	4.1	X	0.148	X	0.174	0.161	1.0
	4.2	1.5X	0.222	1.25X	0.217	0.22	
	4.3	1.75X	0.259	1.25X	0.217	0.238	
	4.4	1.5X	0.222	1.25X	0.217	0.22	
	4.5	X	0.148	X	0.174	0.161	
5. Promote Individual Work Ethic	5.1	2.5X	0.417	2.5X	0.417	0.417	1.0
	5.2	X	0.167	X	0.167	0.167	
	5.3	X	0.167	X	0.167	0.167	
	5.4	1.5X	0.250	1.5X	0.250	0.25	
6. Maximize Data Integrity	6.1	2X	0.444	X	0.333	0.389	1.0
	6.2	1.5X	0.333	X	0.333	0.333	
	6.3	X	0.222	X	0.333	0.278	
7. Enhance Integrity of Business Processes	7.1	1.5X	0.333	2.25X	0.360	0.347	1.0
	7.2	X	0.222	X	0.160	0.191	
	7.3	2X	0.444	3X	0.480	0.462	
8. Maximize Privacy	8.1	1.75X	0.194	X	0.125	0.16	1.0
	8.2	1.75X	0.194	1.25X	0.156	0.175	
	8.3	X	0.111	1.75X	0.219	0.165	
	8.4	3X	0.333	3X	0.375	0.354	
	8.5	1.5X	0.167	X	0.125	0.146	
9. Maximize Organizational Integrity	9.1	1.5X	0.273	X	0.250	0.261	1.0
	9.2	1.5X	0.273	X	0.250	0.261	
	9.3	1.5X	0.273	X	0.250	0.261	
	9.4	X	0.182	X	0.250	0.216	

After determining the local weights for each second tier objective, the weights for the first tier objectives were found. To simplify the conceptual process of swing weighting the first tier objectives shown in Table 4.1, a conceptual hierarchy was presented to the respondents. Figure 4.2 illustrates this conceptual hierarchy along with indicating the X values that were obtained from each respondent.

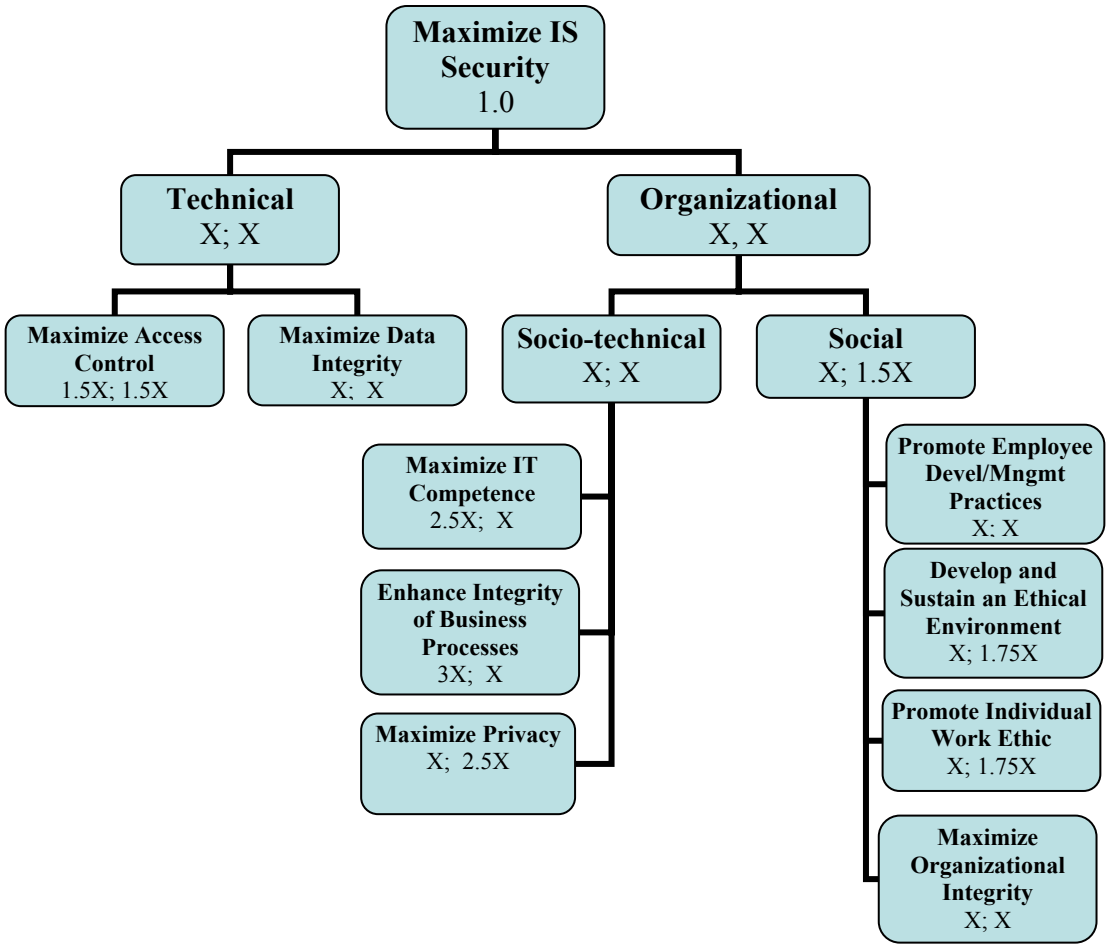

Figure 4.2: Conceptual Hierarchy for the 9 Fundamental Objectives Used for Swing Weighting

As shown in Figure 4.2, rather than asking the respondents to attempt to weight 9 fundamental objectives against each other, the respondents were asked to consider technical, social, and socio-technical objectives by themselves. These categories emerged as a result of what was learned in earlier interviews with the Team. That is, the Team quickly recognized that both technical and organizational objectives were present as fundamental objectives. The Team then recognized that the organizational objectives could be further divided into the two categories of social and socio-technical.

The technical objectives shown in Figure 4.2 were defined as those that required technical expertise to implement and to monitor. That is, the issues of access control and data integrity requires a certain amount of technical expertise from both the IT department to implement and from various managers throughout the organization to monitor. Social objectives were then defined as those that required managerial and organizational expertise to implement and to monitor. For example, to "develop and sustain an ethical environment" does not require any technical expertise from the IT department. And socio-technical objectives were defined as those that required a combination of both technical and organizational expertise to implement and to monitor.

Table 4.14 synthesizes the results from above. As shown in Table 4.14, the Team determined that organizational and technical objectives were equally weighted. However, because there were seven organizational objectives and only two technical objectives, the final global weights for second tier technical objectives were much higher than the final global weights for the second tier organizational objectives. For example, via this weighting scheme, the global weight of objective 6.1, "ensure that inappropriate changes

Table 4.14: Local and Global Weights for the Amended Value Hierarchy

		First Tier	Local Weight	Second Tier	Local Weight	Global Weight
Organizational Weight = 0.5	Socio-technical Weight = 0.45	1. Maximize IT Competence	0.299	1.1	0.140	0.009
				1.2	0.140	0.009
				1.3	0.175	0.012
				1.4	0.228	0.015
				1.5	0.317	0.021
		7. Enhance Integrity of Business Processes	0.34	7.1	0.347	0.027
				7.2	0.191	0.015
				7.3	0.462	0.035
		8. Maximize Privacy	0.361	8.1	0.160	0.013
				8.2	0.175	0.014
				8.3	0.165	0.013
				8.4	0.354	0.029
				8.5	0.146	0.012
	Social Weight = 0.55	2. Promote Employee Development and Management Practices	0.216	2.1	0.250	0.015
				2.2	0.250	0.015
				2.3	0.250	0.015
				2.4	0.250	0.015
		3. Develop and Sustain an Ethical Environment	0.284	3.1	0.206	0.016
				3.2	0.339	0.026
				3.3	0.156	0.012
				3.4	0.300	0.023
		5. Promote Individual Work Ethic	0.284	5.1	0.417	0.033
				5.2	0.167	0.013
				5.3	0.167	0.013
				5.4	0.250	0.020
		9. Maximize Organizational Integrity	0.216	9.1	0.261	0.016
				9.2	0.261	0.016
				9.3	0.261	0.016
				9.4	0.216	0.013
Technical Weight = 0.5	NA	4. Maximize Access Control	0.47	4.1	0.161	0.038
				4.2	0.220	0.052
				4.3	0.238	0.056
				4.4	0.220	0.052
				4.5	0.161	0.038
		6. Maximize Data Integrity	0.53	6.1	0.389	0.103*
				6.2	0.333	0.088
				6.3	0.278	0.074
						Sum = 1.000

*This global weight = 0.5 * 0.53 * 0.389

to data are minimized," equals 0.103. In contrast, the global weight for objective 2.1, "create an environment that promotes contribution," equals 0.015. In other words, any alternatives or tasks associated with objective 6.1 will be given 6.9 times (0.103/0.015) more value than any alternatives or tasks associated with objective 2.1.

4.5 Generate and Score Alternatives (Tasks)

The major advantage of VFT is that it encourages the development of creative alternatives. In past VFT studies (Merrick and Garcia, 2004; Chambal et al., 2003), several alternatives are usually identified via this process and are then analyzed to choose the best alternative from the group. For a simple example, if this process were used to determine what type of degree a particular college student should obtain, an objectives hierarchy similar but much smaller than the one shown in Table 4.1 would be created and might render alternatives such as engineering or accounting degrees. The VFT process would then be used to determine which of these alternatives would be the best choice in terms of meeting all of the objectives to the highest potential.

However, because IS Security is a complex issue that crosses several technical and organizational boundaries, no individual alternative could ever aspire to meet all of the fundamental objectives shown in Table 4.1. Thus for the purposes of this research, the notion of creating single alternatives was replaced with creating individual tasks or a collection of tasks that could be used to attain or implement the various objectives shown in Table 4.1. After these individual tasks are identified and scored, this research then analyzes these tasks against each other to determine a ranking. In other words, this

research conducts a deterministic analysis in Chapter 5 where the results of this analysis will be used to guide MSI Corp in determining the many tasks that are required to maximize IS security and will emphasize the tasks that this research has determined to be the most important via MSI Corp's values.

To generate tasks, the finalized objectives hierarchy shown in Table 4.1 forces appropriate value-driven questions to be asked to accurately determine the various evaluation measures and value functions for the various objectives. Via this process, tasks were naturally considered. To identify and organize these tasks, task generation tables (See Appendix B) were created and given to each member of the Team. Table 4.15 illustrates an example of one task generation table for the fundamental objective "Enhance Integrity of Business Processes."

Table 4.15: Example of a Task Generation Table

Objective	Sub-Objective	Tasks
Enhance integrity of business processes	Understand the expected use of available information and its relation to individual business processes	Task A Task B
	Develop procedures for managing changes to business processes	Task C Task D
	Ensure that appropriate organizational controls are in place	Task E Task F

Each member of the Team was then asked to review the various sub-objectives of each of the task generation tables for all of the fundamental objectives. For each sub-objective, each member of the Team was then asked to review the means objectives

hierarchy in Table 2.2 and to then write down as many tasks as came to mind that could be used to attain or implement an individual sub-objective. After all of the tasks for each of the sub-objectives were written down, the task generation tables for each of the members of the Team were then collected and organized and redundant tasks were removed.

After the tasks were organized, the next step was to score the various tasks against their appropriate evaluation measures using the value functions shown in Appendix C. That is, each alternative received a score that ranged from the lowest to highest possible score for each evaluation measure (0.0 – 1.0). To determine these scores, the Team was brought together and considered each task for a particular measure before advancing to the next task. In most cases, the Team arrived at a consensus for each score for the various tasks. However, when consensus was not found, the average score for the three members of the Team was calculated.

The remainder of this section indicates and discusses the various tasks for each of the fundamental objectives along with illustrating their various scores. To organize the following presentation of results, the fundamental objectives will be presented via the conceptual hierarchy shown in Table 3.3. Additionally, because of the large number of tasks that were created via this research, individual tasks will only be briefly discussed in Chapter 4. A more detailed discussion including the relative importance of these tasks will be given in Chapter 5.

4.5.1 Technical Objectives

As shown in Figure 4.2, the technical objectives consisted of "Maximize Access Control" and "Maximize Data Integrity." Tables 4.16 and 4.17 illustrate the various tasks and scores for these two fundamental objectives. As shown in Tables 4.16 and 4.17, each task was scored individually and a group score was given for each sub-objective. Group scores represent the level of attainment if all of the various tasks for an individual sub-objective were to be implemented. In all cases, group scores were higher than individual scores. In other words, it was found that various sub-objectives could be attained to a better degree via the implementation of multiple tasks.

Additionally, the Team was reluctant to give perfect scores for most individual or group scores due to the technical nature of these objectives. However, as shown in Tables 4.16 and 4.17, a perfect group score of 1.0 was given to sub-objectives 4.5 and 6.3 as these objectives were more managerial in nature. In other words, the Team felt that managerial type objectives could be attained to a full degree whereas with technical type objectives, perfect attainment is not realistic.

4.5.1.1 Maximize Access Control

As shown in Table 4.16, to "maintain personal accountability for system use" the Team derived three tasks. First, security awareness training (T1) would provide employees with a better knowledge of the importance of personal accountability for system use. As shown in Tables 4.16 and 4.17, the Team indicted that T1 would impact all of the sub-objectives (4.1-4.5 and 6.1-6.3) as well. That is, making users aware of the issues surrounding the various sub-objectives for both access control and data integrity

and their importance to IS security is the first step in attainment of these sub-objectives. Second, limiting the use of group accounts or generic IDs (T2) would provide a better ability for system logs to be accurate in terms of identifying users. However, the Team indicated that some group accounts and generic IDs are required for various business activities thus T2 only scored a 0.5. Additionally, the Team indicated that T2 would impact sub-objective 4.2. And finally, password controls that force unique logons (T3) were found to be important as they would help to ensure that users can be identified properly.

To "ensure appropriate levels of user access" the Team derived three additional or unique tasks. First, pre-defined roles and rights (T4) would serve as a guide for indicating what users should be allowed to access what information. As shown in Table 4.16, T4 impacted sub-objective 4.4 as well. Second, authorization procedures (T5) should be created for various levels of information where the levels of authorization would be a function of information sensitivity. And finally, centralized system administration (T6) should be implemented so that user activity can be tracked in an efficient manner.

To "ensure appropriate physical security" the Team derived three unique tasks. First, badges and key cards (T7) would serve to limit physical access to authorized individuals only. Second, video surveillance (T8) would serve to provide a deterrent against unauthorized individuals attempting to gain access to areas that are off limits. And finally, security guards (T9) should be used to monitor and enforce organizational rules for physical security.

Table 4.16: Tasks and Scores for Maximize Access Control

Maximize Access Control			
Sub-Objective	**Task**	**Score**	**Group Score**
4.1 Maintain personal accountability for system use	T1 – Security Awareness Training	0.7	**0.9**
	T2 - Limit the use of group accounts or generic IDs	0.5	
	T3 - Password controls to force unique logons	0.7	
4.2 Ensure appropriate levels of user access	**T1 – Security Awareness Training**	0.7	**0.9**
	T2 - Limit the use of group accounts or generic IDs	0.3	
	T4 - Pre-defined roles and rights	0.7	
	T5 – Authorization procedures	0.7	
	T6- Centralized system administration	0.5	
4.3 Ensure appropriate physical security	**T1 – Security Awareness Training**	0.5	**0.7**
	T7 – Badges/key cards	0.7	
	T8 - Video surveillance	0.5	
	T9 - Security guards	0.7	
4.4 Ensure user access is based on "need to know"	**T1 – Security Awareness Training**	0.7	**0.8**
	T4 – Pre-defined roles and rights	0.5	
	T10 - Well-defined job descriptions	0.5	
	T11 – Segregation of duties matrix	0.5	
	T12 - Automated access monitoring system	0.7	
4.5 Ensure adequate management oversight of access control	**T1 – Security Awareness Training**	0.7	**1**
	T13 - Periodic review of user access roles and rights	0.7	
	T14 – Technical security administration group (policy makers)	0.7	
	T15 – Audit log reviews	0.5	
	T16 - Review of termination lists (centralized review)	0.5	

*** Non-bolded tasks indicate the first time a particular task has been shown**

To "ensure user access is based on 'need to know'" the Team derived 3 unique tasks. First, well-defined job descriptions (T10) would serve as a basis for indicating the types of information that is required for various types of employees. Second, a segregation of duties matrix (T11) should be created that links various duties to the types

of information required. And finally, an automated access monitoring system should be used that tracks and logs access use where the segregation of duties matrix could be used to flag undesired usage patterns.

And finally, as shown in Table 4.16, to "ensure adequate management oversight of access control" four unique tasks were derived. First, a periodic review of user access roles and rights (T13) is required to ensure that as organizational changes are made access control is updated. Second, a security administration group (T14) is required that updates and makes known the various policies associated with access control. Third, audit log reviews (T15) are required to determine if any access breaches have been made and to provide insight into how well information systems are working in terms of access control. And finally, a periodic review of termination lists (T16) is required to determine if any terminated employees are still attempting to access various systems.

4.5.1.2 Maximize Data Integrity

As shown in Table 4.17, many of the same tasks used for the objective "Maximize Access Control" were used for "Maximize Data Integrity." In fact, for the sub-objective "minimize inappropriate changes to data" no new tasks were found. In other words, minimizing inappropriate changes to data is certainly an access control issue.

However, to "ensure appropriate data integrity controls for the processing of data" two new tasks were derived. First, edit and validation routines (T17) are required that provide and enforce the notion that appropriate authorities are making changes to data and to determine if these changes are valid. And second, if errors are found, then

reconciliation procedures (T18) are required to ensure that inappropriate changes to data are reconciled.

To "ensure adequate management oversight of data integrity issues" two new tasks were derived. First, periodic error log audits (T19) are required to determine if edit and validation routines are working properly and to provide insight into the formulation of new data integrity policies. And second, a periodic review of reconciliations (T20) is required to determine if data that has been inappropriately changed has in fact been corrected to its appropriate state.

Table 4.17: Tasks and Scores for Maximize Data Integrity

Maximize Data Integrity			
Sub-Objective	**Task**	**Individual Score**	**Group Score**
6.1 Minimize inappropriate changes to data	**T1 – Security Awareness Training**	0.7	**0.8**
	T4 - Pre-defined roles and rights	0.5	
	T10 - Well-defined job descriptions	0.5	
	T11 – Segregation of duties matrix	0.5	
	T12 - Automated access monitoring system	0.7	
	T5 - Authorization procedures	0.7	
6.2 Ensure appropriate data integrity controls for the processing of data	**T1 – Security Awareness Training**	0.5	**0.9**
	T17 - Edit and validation routines	0.8	
	T18 – Reconciliation procedures	0.7	
6.3 Ensure adequate management oversight of data integrity issues	**T1 – Security Awareness Training**	0.7	**1**
	T14 – Technical security administration group (policy makers)	0.7	
	T19 – Periodic error log audits	0.7	
	T20 – Periodic review of reconciliations	0.7	

*** Non-bolded tasks indicate the first time a particular task has been shown**

4.5.2 Socio-Technical Objectives

As shown in Figure 4.2, the socio-technical objectives consisted of "Maximize IT Competence," "Enhance Integrity of Business Processes" and "Maximize Data Privacy." Tables 4.18-4.20 illustrate the various tasks and scores for these three fundamental objectives. As discussed earlier, the socio-technical objectives were defined as those that required a combination of both technical and organizational (social) expertise to implement and to monitor. Thus it should be no surprise that the tasks shown in Tables 4.18-4.20 do in fact consist of both technical and social elements.

4.5.2.1 Maximize IT Competence

As shown in Table 4.18, to "develop a management team that leads by example" the Team derived five new tasks. First, creating amendments (T21) to MSI Corp's Guiding Principles (See Section 4.2) that specifically indicate the desire for management teams to lead by example helps to create a corporate culture that employees in the entire organization understand and follow. Second, the Team felt that amendments (T22) should be made to MSI Corp's Code of Business Conduct and Ethics (See Section 4.2) policy as well. Since MSI Corp requires employees to periodically review and take a test on this policy, the notion of management teams leading by example is reinforced. Third, the Team decided that the notion of management teams leading by example should be written explicitly in managerial job descriptions (T23). Fourth, compensation and incentive programs should be designed to influence management teams leading by example. And finally, empowerment training (T25) should be introduced to managers to

indicate how leading by example empowers subordinates thus making the manger's output more efficient.

Table 4.18: Tasks and Scores for Maximize IT Competence

Maximize IT Competence			
Sub-Objective	**Tasks**	**Individual Score**	**Group Score**
1.1 Develop a management team that leads by example	T21- Amendments to Guiding Principles	0.5	**0.9**
	T22 - Amendments to Code of Business Conduct and Ethics	0.7	
	T23 – Written in Job Descriptions	0.7	
	T24 - Compensation/incentive programs designed to influence management teams leading by example	0.7	
	T25 -Empowerment Training	0.7	
1.2 Ensure confidence/comfort level in using computers	T26 - IT Training and development	0.7	**0.8**
	T27 – Hire employees with adequate IT skills	0.5	
	T28 - Standardized computer platforms	0.5	
1.3 Create legitimate opportunities for financial gain	T29 - Compensation programs aligned with company values	0.8	**0.8**
	T30 - Recognition programs	0.3	
	T31 - Goals and incentives tied to job descriptions and performance	0.7	
1.4 Ensure employees have adequate IT training	**T26 – IT Training and development**	0.7	**0.9**
	T32 - Skills assessments and performance evaluations	0.5	
	T33 - Individual development plans	0.7	
	T34 – Budget for Training	0.7	
1.5 Ensure IT capability level of staff	**T26 – IT Training and development**	0.7	**1**
	T27 – Hire employees with adequate IT skills	0.5	
	T32 - Skills assessments and performance evaluations	0.8	
	T33 - Individual development plans	0.7	

*** Non-bolded tasks indicate the first time a particular task has been shown**

To "ensure confidence/comfort level in using computers" the Team derived three new tasks. First, the Team undoubtedly decided that computer training and development courses (T26) should be offered. As shown in Table 4.18, T26 impacted sub-objectives 1.4 and 1.5 as well. Second, the Team indicated that hiring policies (T26) should be created that require all new employees to have a certain degree of computer skills. As shown in Table 4.18, T27 was found to impact sub-objective 1.5 as well. And finally, the Team indicated that MSI Corp should standardize computer platforms (T28) throughout the entire organization to limit the amount of confusion that ultimately exists when multiple skill sets are required for multiple platforms.

To "create legitimate opportunities for financial gain" the Team derived three new tasks. First, providing compensation programs that are aligned with company values (T29) ensures that employees who adhere to corporate objectives are adequately compensated. Second, recognition programs (T30) should be provided so that employees who work hard and are profitable to the organization are recognized in an esteemed fashion. And finally, goals and incentives should be tied to job descriptions thus making these goals and incentives attainable.

To "ensure employees have adequate IT training" the Team derived three new tasks. First, skills assessments and performance evaluations (T32) should be periodically conducted to determine if past training exercises have been worthwhile and to determine what type of training may be required in the future. As shown in Table 4.18, T32 was found to impact sub-objective 1.5 as well. Second, individual development plans (T33) should be created and followed that aspires to bring various employees up to speed in

terms of current technical expertise required for particular job functions. As shown in Table 4.18, T33 was found to impact sub-objective 1.5 as well. That is, individual development plans should impact the technical capability level of employees. And finally, via assessments and development plans, adequate budgets for training (T34) should be created and followed.

4.5.2.2 Enhance Integrity of Business Processes

As shown in Table 4.19, to "understand the expected use of available information and its relation to individual business processes" the Team derived three new tasks. First, process design training (T30) should be implemented so that employees understand the various business processes of the organization and the types of information that are required as inputs and outputs to these processes. As shown in Table 4.19, T35 impacted sub-objectives 7.2 and 7.3 as well. Second, all business processes should be documented and made known (T36) to employees so that everyone in the organization can enhance their knowledge on the expected use of information. And finally, procedures for classifying information (T37) in terms of sensitivity and ownership and making these classifications known to the entire organization should be implemented.

To "develop procedures for managing changes to business processes" the Team derived two new tasks. First, a program (T38) should be created that manages business process improvement. And second, a business process maturity/lifecycle model should be created (T39) and made known to provide employees a template for understanding how their various day-to-day activities impact the organization as a whole.

Table 4.19: Tasks and Scores for Enhance Integrity of Business Processes

Enhance Integrity of Business Processes			
Sub-Objective	**Tasks**	**Individual Score**	**Group Score**
7.1 Understand the expected use of available information and its relation to individual business processes	T35 - Process design training	0.7	**0.7**
	T36 - Document and make known business processes	0.5	
	T37 -Create and make known information classification standards	0.5	
7.2 Develop procedures for managing changes to business processes	**T35 – Process design training**	0.7	**0.8**
	T38 - Create and manage a business process improvement program	0.7	
	T39 - Create and adhere to business process maturity/lifecycle model	0.7	
7.3 Ensure that appropriate organizational controls are in place	**T35 - Process design training**	0.7	**0.9**
	T40 - Risk assessment activities	0.7	
	T41 - Periodic review of business process improvement program	0.7	
	T42 -Executive management oversight	0.7	

*** Non-bolded tasks indicate the first time a particular task has been shown**

And finally, to "ensure that appropriate organizational controls are in place" three new tasks were derived. First, the Team recognized that risk assessment activities (T40) should be carried out to understand the impact and subsequent risk associated with inefficient or deleterious business processes. Second, a periodic review of the business process improvement program (T41) should be conducted that aspires to determine if any changes to this program are required. And finally, due to the importance of creating and maintaining efficient business process implementation, the Team decided that executive

managers should be required to keep a keen eye on the organizational control of business processes.

4.5.2.3 Maximize Privacy

As shown in Table 4.20, several tasks that have previously been discussed (T1, T2-T9, T21, and T22) impact the various sub-objectives for maximizing privacy. Not surprisingly, the presence of the more technical task, security awareness training (T1), undoubtedly impacts most of these sub-objectives as privacy issues are certainly technical in nature. Thus technical training and awareness programs are required. The tasks T2-T9 deal with access control and physical security and are shown in Table 4.20 to impact the sub-objective "ensure that sensitive data is adequately secured." And the presence of the more social tasks T21 and T22 are required to emphasize the importance of data privacy, disclosure agreements, and repercussions of disclosure of sensitive data.

However, several new tasks were derived for maximizing privacy. The new tasks of creating amendments to the employee manual (T43) and placing posters in the coffee room (T44) were shown to impact the sub-objectives that dealt with emphasizing the importance of data privacy, disclosure agreements, and repercussions of disclosure of sensitive data. And the new task of creating a nondisclosure agreement with repercussions (T45) was shown to obviously impact sub-objectives 8.2 and 8.3.

Table 4.20: Tasks and Scores for Maximize Privacy

Maximize Privacy			
Sub-Objective	**Tasks**	**Score**	**Group Score**
8.1 Emphasize importance of data privacy	**T1 – Security Awareness Training**	0.7	**1**
	T21- Amendments to Guiding Principles	0.5	
	T22 - Amendments to Code of Business Conduct and Ethics	0.7	
	T43 - Amendments to Employee Manual	0.7	
	T44 – Posters in the coffee room	0.5	
8.2 Ensure employee awareness against disclosure of sensitive data	**T1 – Security Awareness Training**	0.7	**1**
	T21- Amendments to Guiding Principles	0.5	
	T22 - Amendments to Code of Business Conduct and Ethics	0.7	
	T43 - Amendments to Employee Manual	0.7	
	T44 - Posters in the coffee room	0.5	
	T45 – Nondisclosure agreement with repercussions	0.9	
8.3 Ensure employees understand the repercussions of disclosing sensitive data	**T1 – Security Awareness Training**	0.7	**1**
	T21- Amendments to Guiding Principles	0.5	
	T22 - Amendments to Code of Business Conduct and Ethics	0.7	
	T43 - Amendments to Employee Manual	0.7	
	T44 - Posters in the coffee room	0.5	
	T45 – Nondisclosure agreement with repercussions	0.9	
8.4 Ensure that sensitive data is adequately secured	**T1 – Security Awareness Training**	0.5	**0.8**
	T2 - Limit the use of group accounts or generic IDs	0.7	
	T3 - Password controls to force unique logons	0.7	
	T4 - Pre-defined roles and rights	0.5	
	T5 - Authorization procedures	0.7	
	T6- Centralized system administration	0.8	
	T7 – Badges/key cards	0.7	
	T8 - Video surveillance	0.7	
	T9 - Security guards	0.7	
8.5 Ensure adequate management oversight of privacy issues	**T1 – Security Awareness Training**	0.7	**1**
	T14 - Security administration group/policy makers	0.7	
	T46 - Privacy officer	0.7	
	T47 - Incident response team	0.7	
	T48 - Periodic review of public information	0.5	
	T49 - Oversee Privacy aspects of Security Awareness Training	0.7	

*** Non-bolded tasks indicate the first time a particular task has been shown**

Additionally, to "ensure adequate management oversight of privacy issues" four new and unique tasks were created. First, a dedicated privacy officer (T46) position should be created. Second, an incident response team (T47) should be created and led by the privacy officer. Third, the privacy officer should periodically review the sensitivity of public information (T48) to determine if access constraints are required. And finally, the privacy officer should periodically oversee that the privacy aspects of the security awareness training program (T49) are working properly.

4.5.3 Social Objectives

As shown in Figure 4.2, the social objectives consisted of "Promote Employee Development and Management Practices," "Develop and Sustain an Ethical Environment," "Promote Individual Work Ethic," and "Maximize Organizational Integrity." Tables 4.21-4.24 illustrate the various tasks and scores for these four fundamental objectives. As discussed earlier, social objectives were defined as those that required managerial and organizational expertise to implement and to monitor. Thus it should be no surprise that the tasks shown in Tables 4.21-4.24 are in fact mostly social in nature. Additionally, higher scores are shown for these social objectives as the Team felt that managerial and organizational type issues could be attained to a higher degree than the more technical objectives. And finally, as shown in Tables 4.21-4.24, most of the new tasks created for the social objectives impact most if not all of the various sub-objectives in this group. Thus even though global weights for many of these sub-objectives are much lower than the global weights for the technical objectives, final

value-adjusted scores (See Section 3.3.8 for clarification) will be much higher than one might expect.

4.5.3.1 Promote Employee Development and Management Practices

As shown in Table 4.21, eight new tasks (T50-T57) were derived for the sub-objectives of promoting employee development and management practices. First, a written document that explains to managers the importance of authority delegation and its ability to empower employees (T50) should be created. As shown in Table 4.21, empowering employees impacts issues concerning increasing morale (sub-objective 2.2), increasing pride (sub-objective 2.3), and developing a motivated workforce (sub-objective 2.4) as well.

Similarly, tasks T51-T57 were shown to all have an impact on promoting contribution, instilling high levels of morale, increasing pride, and developing a motivated workforce. These tasks included: making sure that compensation and incentives are tied to performance (T51); a rewards program (T52); ensuring well-defined career paths (T53); creating open communication policies (T54); creating and maintaining well-defined contribution/matching programs (T55); conducting periodic teambuilding exercises (T56); and providing training and development programs for career advancement (T57).

Table 4.21: Tasks and Scores for Promote Employee Development and Management Practices

Sub-Objective	Tasks	Ind. Score	Group Score
2.1 Create an environment that promotes contribution	**T21- Amendments to Guiding Principles**	0.5	1.0
	T50 - Authority delegation (written document for empowerment)	0.9	
	T51 – Compensation and incentives tied to performance	0.9	
	T52 - Rewards program tied to employee performance	0.7	
	T53 – Well-defined career paths	0.5	
	T54 - Open communication policy	0.7	
	T55 - Contribution/matching program	0.7	
	T56 – Teambuilding Exercises	0.7	
	T57 - Provide training and development programs for career advancement	0.5	
2.2 Instill high levels of morale	**T21- Amendments to Guiding Principles**	0.7	1.0
	T50 - Authority delegation (written document for empowerment)	0.9	
	T51 - Compensation and incentives tied to performance	0.8	
	T52 - Rewards program tied to employee performance	0.8	
	T53 – Well-defined career paths	0.7	
	T54 - Open communication policy	0.5	
	T55 – Contribution/matching program	0.7	
	T56 – Teambuilding Exercises	0.5	
	T57 - Provide training and development programs	0.6	
2.3 Increase/maintain pride in the organization	**T21- Amendments to Guiding Principles**	0.7	0.9
	T50 - Authority delegation	0.7	
	T51 - Compensation and incentives tied to performance	0.7	
	T52 - Rewards program tied to employee performance	0.7	
	T53 – Well-defined career paths	0.5	
	T54 - Open communication policy	0.5	
	T55 – Contribution/matching program	0.7	
	T56 – Teambuilding Exercises	0.7	
	T57 - Provide training and development programs for career advancement	0.6	
2.4 Develop and maintain a motivated workforce	**T21- Amendments to Guiding Principles**	0.5	1.0
	T50 - Authority delegation (written document for empowerment)	0.5	
	T51 - Compensation and incentives tied to performance	0.5	
	T52 - Rewards program tied to employee performance	0.9	
	T53 – Well-defined career paths	0.8	
	T54 - Open communication policy	0.7	
	T55 – Contribution/matching program	0.8	
	T56 - Teambuilding Exercises	0.5	
	T57 - Provide training and development programs for career advancement	0.8	

*** Non-bolded tasks indicate the first time a particular task has been shown**

4.5.3.2 Develop and Sustain an Ethical Environment

As shown in Table 4.22, eight new tasks (T58-T65) were derived for the sub-objectives of developing and sustaining an ethical environment. To "create an environment that makes it okay to report unethical behavior " the Team derived two new tasks that included establishing a hotline (T58) and creating and making known a policy of no retaliation against employees who report suspected issues. To "instill professional-based work ethics" the Team derived one new task that included creating hiring policies that include background and credit checks (T59) in an attempt to limit unethical employees from entering MSI Corp.

To "ensure adequate management oversight of developing and sustaining an ethical environment" the Team derived five new tasks. First, the Team indicated that a chief ethics officer (T61) should be appointed who oversees and maintains policies related to maintaining an ethical environment. Second, the Team indicated that the ethics officer should be responsible for calling together meetings via appointed ethics committee (T62) members. Third, the Team indicated that various findings of ethics committee meetings should be directly reported to the board of directors (T63) or some type of audit committee for review. Fourth, the Team indicated that a periodic and random questionnaire (T64) should be created and administered to employees to determine how effective current policies have been in terms of sustaining an appropriate ethical environment. And finally, the Team indicated that a written test should be created and maintained that periodically is given to employees that covers various ethics policies.

Table 4.22: Tasks and Scores for Develop and Sustain an Ethical Environment

Sub-Objective	Tasks	Individual Score	Group Score
3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	**T21- Amendments to Guiding Principles**	0.5	1.0
	T22 - Amendments to Code of Business Conduct and Ethics	0.6	
	T58 – Hotline	0.9	
	T59 - Policy of no retaliation to employees who report suspected issues	0.7	
3.2 Instill professional-based work ethics	**T21- Amendments to Guiding Principles**	0.7	0.8
	T22 - Amendments to Code of Business Conduct and Ethics	0.5	
	T60 - Hiring policies (background and credit checks)	0.7	
3.3 Create an environment that promotes organizational loyalty	**T21- Amendments to Guiding Principles**	0.5	0.9
	T50 - Authority delegation (written document for empowerment)	0.5	
	T51 - Compensation and incentives tied to performance	0.7	
	T52 - Rewards program tied to employee performance	0.7	
	T53 – Well-defined career paths	0.3	
	T54 - Open communication policy	0.3	
	T55 - Contribution/matching program	0.5	
	T56 - Teambuilding Exercises	0.5	
	T57 - Provide training and development programs for career advancement	0.7	
3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	T61 - Chief Ethics Officer	0.8	1.0
	T62 - Ethics Committee	0.8	
	T63 - Ethics officer reports to the board or audit committee	0.7	
	T64 - Periodic ethics questionnaires of employees	0.7	
	T65 - Employees reaffirm (written test) ethics policy on a periodic basis	0.7	

*** Non-bolded tasks indicate the first time a particular task has been shown**

4.5.3.3 Promote Individual Work Ethic

As shown in Table 4.23, there were no additional tasks created for the sub-objectives for promoting individual work ethic. This was due to the fact that many of the tasks related to creating an ethical environment could also be used to attain many of the sub-objectives for promoting individual work ethic. However, as shown in Table 4.23, scores were generally lower for this social objective. This was due to the fact that an organization should be able to do a good job of creating an ethical environment, yet whether or not all individuals will actually be positively influenced by this environment must be questioned. In other words, as one of the respondents stated, "You can lead a horse to water, but you can't make him drink."

Table 4.23: Tasks and Scores for Promote Individual Work Ethic

Sub-Objective	Tasks	Ind. Score	Group Score
5.1 Maximize employee integrity in the company	**T21- Amendments to Guiding Principles**	0.5	0.8
	T22 - Amendments to Code of Business Conduct and Ethics	0.5	
	T50 - Authority delegation (written document for empowerment)	0.5	
	T51 - Compensation and incentives tied to performance	0.5	
	T52 - Rewards program tied to employee performance	0.7	
	T53 – Well-defined career paths	0.5	
	T54 – Open communication policy	0.7	
	T55 - Contribution/matching program	0.5	
	T57 - Provide training and development programs for career advancement	0.8	
5.2 Create a desire to not jeopardize the reputation of the company	**T21- Amendments to Guiding Principles**	0.5	0.8
	T22 - Amendments to Code of Business Conduct and Ethics	0.5	
	T45 – Nondisclosure agreement with repercussions	0.7	
	T50 - Authority delegation (written document for empowerment)	0.5	
	T51 - Compensation and incentives tied to performance	0.5	
	T52 - Rewards program tied to employee performance	0.7	
	T53 – Well-defined career paths	0.4	
	T54 – Open communication policy	0.5	
	T55 - Contribution/matching program	0.5	
	T56 - Teambuilding Exercises	0.3	
	T57 - Provide training and development programs for career advancement	0.3	
5.3 Create an environment that promotes the organization 's best interests rather than personal gain	**T21- Amendments to Guiding Principles**	0.7	0.9
	T22 - Amendments to Code of Business Conduct and Ethics	0.7	
	T45 – Nondisclosure agreement with repercussions	0.7	
	T51 - Compensation and incentives tied to performance	0.7	
	T52 - Rewards program tied to employee performance	0.8	
	T53 – Well-defined career paths	0.5	
	T55 - Contribution/matching program	0.7	
	T56 - Teambuilding Exercises	0.5	
	T57 - Provide training and development programs for career advancement	0.5	
5.4 Minimize temptation to use information for personal benefit	**T1 – Security Awareness Training**	0.7	0.8
	T5 - Authorization procedures	0.5	
	T21- Amendments to Guiding Principles	0.5	
	T22 - Amendments to Code of Business Conduct and Ethics	0.5	
	T45 – Nondisclosure agreement with repercussions	0.7	
	T51 - Compensation and incentives tied to performance	0.5	
	T55 - Contribution/matching program	0.5	

*** Non-bolded tasks indicate the first time a particular task has been shown**

4.5.3.3 Maximize Organizational Integrity

As shown in Table 4.24, four new tasks (T66-T69) were derived for the sub-objectives of maximizing organizational integrity. To "create an environment that promotes respect" the Team derived one new task that included offering a function for subordinates to provide upward feedback to managers (T66). Obviously, if done in the right manner, being able to provide upward feedback could serve to establish a stronger and mutually respectful relationship between managers and subordinates. On the other end, to "create an environment that promotes individual reliability" subordinates must be evaluated in terms of performance (T67) as well.

To "ensure adequate management oversight of organizational integrity issues" two new tasks were derived. First, periodic budget and financial reviews (T68) should be conducted to determine if organizational integrity has been maximized or whether new policies are needed. And second, the Team indicated that a periodic review of business plans via the Board of Directors and a specialized Audit Committee is required to determine if business plans are being kept in line with organizational objectives.

Table 4.24: Tasks and Scores for Maximize Organizational Integrity

Sub-Objective	Tasks	Individual Score	Group Score
9.1 Create an environment that empowers employees	**T21- Amendments to Guiding Principles**	0.5	1.0
	T50 - Authority delegation (written document for empowerment)	0.9	
	T51 - Compensation and incentives tied to performance	0.7	
	T53 – Well-defined career paths	0.5	
	T54 – Open communication policy	0.5	
	T57 – Provide training and development programs for career advancement	0.8	
9.2 Create an environment that promotes respect	**T21- Amendments to Guiding Principles**	0.7	1.0
	T22 - Amendments to Code of Business Conduct and Ethics	0.7	
	T50 - Authority delegation (written document for empowerment)	0.7	
	T54 – Open communication policy	0.5	
	T56 - Teambuilding Exercises	0.8	
	T66 - Performance management including upward feedback	0.8	
9.3 Create an environment that promotes individual reliability	**T21- Amendments to Guiding Principles**	0.3	0.9
	T22 - Amendments to Code of Business Conduct and Ethics	0.3	
	T51 - Compensation and incentives tied to performance	0.6	
	T52 - Rewards program tied to employee performance	0.7	
	T53 – Well-defined career paths	0.7	
	T55 - Contribution/matching program	0.7	
	T57 – Provide training and development programs for career advancement	0.8	
	T67 - Performance evaluations	0.8	
9.4 Ensure adequate management oversight of organizational integrity issues	**T61 - Chief Ethics Officer**	0.9	1.0
	T62 - Ethics Committee	0.8	
	T63 - Ethics officer reports to the board or audit committee	0.8	
	T64 - Periodic ethics questionnaires of employees	0.8	
	T68 - Budget/Financial reviews	0.7	
	T69 - Board and Audit Committee periodic review of business plans	0.8	

*** Non-bolded tasks indicate the first time a particular task has been shown**

4.6 Summary

Chapter 4 presented the results of Steps 2-7 as discussed in Chapter 3 via an organizational study with MSI Corp. As was discussed, Dhillon and Torkzadeh's (2006) framework of fundamental objectives (Table 2.1) was used as a starting point to create an amended fundamental objectives hierarchy (Table 4.1) and was altered to match the values of MSI Corp (Step 2). Via the process of creating Table 4.1, an extensive list of evaluation measures (Step 3) and value functions (Step 4) were then determined for each sub-objective.

As the research Team became more and more familiar with these objectives, a conceptual hierarchy (Figure 4.2) then emerged which indicated that the 9 fundamental objectives in Table 4.1 could be categorized into three distinct groups that consisted of technical, socio-technical and social objectives. This conceptual hierarchy was then used as a basis for weighting (Step 5) the various objectives via the swing weighting process.

After weights were determined for the entire objectives hierarchy shown in Table 4.1, tasks were then derived (Step 6) for each of the sub-objectives. As shown in Section 4.5, a total of 69 value-driven tasks were found that could be used to implement or attain the various sub-objectives. These various tasks were then scored (Step 7) relative to the various value functions shown in Appendix C for each of the sub-objectives. In other words, a score (0.0-1.0) indicated the degree to which a specific task could attain a particular sub-objective where several tasks were found to impact several sub-objectives. Chapter 5 will now present a deterministic and sensitivity analysis which will be used to

provide recommendations in the form of indicating the relative importance of these tasks as they relate to the values of MSI Corp for maximizing IS security.

Chapter 5 -Analysis and Discussion of Findings

5.1 Introduction

The purpose of this chapter is to present the results of a deterministic and sensitivity analysis performed on the 69 value-driven security tasks identified in Chapter 4. Particular attention will be given to explaining and organizing these various tasks so that valid recommendations can then be made to MSI Corp in the form of indicating the appropriate actions that should be taken to maximize IS security in their organization. Additionally, the results of the sensitivity analysis will be used to determine how changes in the weights found in Chapter 4 would influence the overall ranking of these tasks.

5.2 Deterministic Analysis

As discussed in Section 3.3.8, to determine a relative ranking of the 69 value-driven tasks, the additive value function is used as shown in Equation 1 (Kirkwood 1997, pg. 230):

$$(1)\quad V(x) = \sum_{i=1}^{n} w_i * v_i(x_i)$$

where $\mathbf{w_i}$ indicates the various global weights for each of the sub-objectives found in Section 4.4 and $\mathbf{v_i(x_i)}$ represents the value-adjusted scores for the various tasks found in Section 4.5.

Table 5.1 illustrates a ranking of the sub-objectives by using global weights (w_i) alone. As shown in Table 5.1, MSI Corp indicated that the technical objectives and their associated sub-objectives held the highest global weights and the socio-technical and social objectives held lower global weights. Specifically, issues surrounding data integrity (Objective 6) were found to be the most important via MSI Corp's value system, and issues surrounding IT Competence (Objective 1) were found to be the least important.

Table 5.1: Rankings of Sub-Objectives by Global Weight

Rank	Second Tier Objective	Type	Local Weight	Global Weight
1	6.1 Ensure that inappropriate changes to data are minimized	**Technical**	0.3889	**0.1031**
2	6.2 Ensure appropriate data integrity controls for the processing of data	**Technical**	0.3333	**0.0883**
3	6.3 Ensure adequate management oversight of data integrity issues	**Technical**	0.2778	**0.0736**
4	4.3 Ensure appropriate physical security	**Technical**	0.2383	**0.056**
5	4.2 Ensure appropriate levels of user access	**Technical**	0.2198	**0.0517**
6	4.4 Ensure user access is based on "need to know"	**Technical**	0.2198	**0.0517**
7	4.1 Ensure personal accountability for system use	**Technical**	0.161	**0.0378**
8	4.5 Ensure adequate management oversight of access control issues	**Technical**	0.161	**0.0378**
9	7.3 Ensure that appropriate organizational controls are in place	**Socio-technical**	0.4622	**0.0354**
10	5.1 Maximize employee integrity in the company	**Social**	0.4167	**0.0325**
11	8.4 Ensure that sensitive data is adequately secured	**Socio-technical**	0.3542	**0.0288**
12	3.2 Develop and/or make known an understood value system in the organization	**Social**	0.3389	**0.0265**
13	7.1 Ensure an understanding of the expected use of available information and its relation to individual business processes	**Socio-technical**	0.3467	**0.0265**
14	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	**Social**	0.3	**0.0234**
15	1.5 Ensure IT capability level of staff	**Socio-technical**	0.3165	**0.0213**

16	5.4 Minimize temptation to use information for personal benefit	**Social**	0.25	**0.0195**
17	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	**Social**	0.2056	**0.0161**
18	9.1 Create an environment that empowers employees	**Social**	0.2614	**0.0155**
19	9.2 Create an environment that promotes respect	**Social**	0.2614	**0.0155**
20	9.3 Create an environment that promotes individual reliability	**Social**	0.2614	**0.0155**
21	1.4 Ensure employees have adequate IT training	**Socio-technical**	0.2278	**0.0153**
22	2.1 Create an environment that promotes contribution	**Social**	0.25	**0.0149**
23	2.2 Instill high levels of morale	**Social**	0.25	**0.0149**
24	2.3 Increase/maintain pride in the organization	**Social**	0.25	**0.0149**
25	2.4 Develop and maintain a motivated workforce	**Social**	0.25	**0.0149**
26	7.2 Develop procedures for managing changes to business processes	**Socio-technical**	0.1911	**0.0146**
27	8.2 Ensure employee awareness against disclosure of sensitive data	**Socio-technical**	0.1753	**0.0142**
28	8.3 Ensure employees understand the repercussions of disclosing sensitive data	**Socio-technical**	0.1649	**0.0134**
29	5.2 Create a desire to not jeopardize the reputation of the company	**Social**	0.1667	**0.013**
30	5.3 Create an environment that promotes the organization's best interests rather than personal gain	**Social**	0.1667	**0.013**
31	8.1 Emphasize importance of data privacy	**Socio-technical**	0.1597	**0.013**
32	9.4 Ensure adequate management oversight of organizational integrity issues	**Social**	0.2159	**0.0128**
33	3.3 Create an environment that promotes organizational loyalty	**Social**	0.1556	**0.0121**
34	1.3 Ensure an adequate understanding of the importance of computer technology and how it is related to the financial well-being of your organization	**Socio-technical**	0.1749	**0.0118**
35	8.5 Ensure adequate management oversight of privacy issues	**Socio-technical**	0.1458	**0.0118**
36	1.1 Develop a management team that leads by example	**Socio-technical**	0.1404	**0.0094**
37	1.2 Ensure confidence/comfort level in using computers	**Socio-technical**	0.1404	**0.0094**

As shown in Table 5.1, sub-objective 6.1, “ensure that inappropriate changes to data are minimized,” was found to be the most important with a global weight of 0.1031; a score significantly higher than all of the other sub-objectives shown in Table 5.1. In other words, of all the issues surrounding IS security, MSI Corp indicated that keeping data in its original and correct form was the most important issue. Of course, this makes sense when considering that without reliable data, an organization would not be able to prosper. Other issues that were at the top of the list included: ensuring appropriate data integrity controls for the processing of data; ensuring adequate management oversight of data integrity issues; ensuring appropriate physical security; ensuring appropriate levels of user access; ensuring user access is based on "need to know;" ensuring personal accountability for system use; and ensuring adequate management oversight of access control issues.

As shown in Table 5.1, the highest ranked socio-technical issue was that of sub-objective 7.3, “ensure that appropriate organizational controls are in place,” and the highest ranked social objective was that of sub-objective 5.1, “maximize employee integrity in the company.” Interestingly enough, both of these sub-objectives dealt with integrity as well; only at a higher level than that of data integrity issues. That is, of all the organizational objectives, MSI Corp found that maintaining the integrity of both business processes and employees were the most important. Other organizational issues that were at the top of the list included: ensuring that sensitive data is adequately secured; developing and/or making known an understood value system in the organization; ensuring an understanding of the expected use of available information and its relation to

individual business processes; ensuring adequate management oversight of developing and sustaining an ethical environment; and ensuring the IT capability level of staff.

However, it should be noted that examining these issues via their global weights alone can be misleading. That is, as shown in Table 4.14, MSI Corp equally weighted the technical and organizational objectives. And because there were only two technical objectives as compared to seven organizational objectives, global weights for the associated technical sub-objectives are naturally higher than those of the organizational sub-objectives. Thus conducting a deterministic analysis for the value-driven tasks using a combination of the value-adjusted score along with the global weight, as shown in Equation 1, provides a more accurate analysis in terms of measures that MSI Corp should focus on for maximizing IS security.

5.2.1 Ranking the 69 Value-Driven Tasks for Maximizing IS Security

Table 5.2 provides a ranking of the 69 value-driven tasks for maximizing IS security using Equation 1. The actual calculations for the final scores are shown in Appendix E. As shown in Table 5.2, the top 10 highest ranked tasks consisted of three technical tasks (T1, T5, and T4) and 7 organizational tasks (T21, T22, T51, T12, T52, T57, T55). Thus global weight alone did not dominate the final rankings of these tasks. In other words, the ranking of a particular task was dependent on how many sub-objectives it impacted, how much global weight is associated with a particular sub-objective it impacted, and how well it scored relative to the sub-objectives it impacted.

Table 5.2: Final Rankings of the 69 Value-Driven Tasks for Maximizing IS Security

Rank	Task	Final Score $\Sigma w_i * v_i(x_i)$
1	T1 – Security Awareness Training	0.3859
2	T21- Amendments to Guiding Principles	0.1583
3	T5 – Authorization procedures	0.1382
4	T4 – Pre-defined roles and rights	0.1280
5	T22 - Amendments to Code of Business Conduct and Ethics	0.1150
6	T51 – Compensation and incentives tied to performance	0.1134
7	T12 - Automated access monitoring system	0.1084
8	T52 - Rewards program tied to employee performance	0.1078
9	T57 - Provide training and development programs for career advancement	0.1070
10	T55 - Contribution/matching program	0.1017
11	T50 - Authority delegation (written document for empowerment)	0.0983
12	T53 – Well-defined career paths	0.0874
13	T35 - Process design training	0.0865
14	T14 - Security administration group/policy makers	0.0862
15	T54 - Open communication policy	0.0841
16	T10 - Well-defined job descriptions	0.0774
17	T11 – Segregation of duties matrix	0.0774
18	T17 - Edit and validation routines	0.0706
19	T56 - Teambuilding Exercises	0.0646
20	T18 – Reconciliation procedures	0.0618
21	T7 – Badges/key cards	0.0594
22	T9 - Security guards	0.0594
23	T45 – Nondisclosure agreement with repercussions	0.0567
24	T2 - Limit the use of group accounts or generic IDs	0.0546
25	T19 – Periodic error log audits	0.0515
26	T20 – Periodic review of reconciliations	0.0515
27	T6- Centralized system administration	0.0489
28	T8 - Video surveillance	0.0482
29	T3 - Password controls to force unique logons	0.0466
30	T61 - Chief Ethics Officer	0.0372
31	T36 - Document and make known business processes	0.0370
32	T37 -Create and make known information classification standards	0.0368
33	T26 - IT Training and development	0.0322
34	T62 – Ethics Committee	0.0290
35	T43 - Amendments to Employee Manual	0.0284
36	T63 – Ethics officer reports to the board or audit committee	0.0266
37	T64 - Periodic ethics questionnaires of employees	0.0266
38	T13 - Periodic review of user access roles and rights	0.0265
39	T33 - Individual development plans	0.0256

40	T40 - Risk assessment activities	0.0248
41	T41 - Periodic review of business process improvement program	0.0248
42	T42 -Executive management oversight	0.0248
43	T32 - Skills assessments and performance evaluations	0.0247
44	T44 - Posters in the coffee room	0.0203
45	T15 – Audit log reviews	0.0189
46	T16 - Review of termination lists (centralized review)	0.0189
47	T65 - Employees reaffirm (written test) ethics policy on a periodic basis	0.0163
48	T27 – Hire employees with adequate IT skills	0.0154
49	T58 – Ethics Hotline	0.0145
50	T66 - Performance management including upward feedback	0.0124
51	T67 - Performance evaluations	0.0124
52	T60 – Hiring policies (background and credit checks)	0.0115
53	T59 - Policy of no retaliation to employees who report suspected issues	0.0113
54	T34 - Budget for Training	0.0107
55	T69 - Board and Audit Committee periodic review of business plans	0.0102
56	T38 - Create and manage a business process improvement program	0.0102
57	T39 - Create and adhere to business process maturity/lifecycle model	0.0102
58	T29 - Compensation programs aligned with company values	0.0094
59	T68 - Budget/Financial reviews	0.0090
60	T31 - Goals and incentives tied to job descriptions and performance	0.0083
61	T46 - Privacy officer	0.0083
62	T47 - Incident response team	0.0083
63	T49 - Oversee Privacy aspects of Security Awareness Training	0.0083
64	T23 - Written in Job Descriptions	0.0065
65	T24 - Compensation/incentive programs designed to influence management teams leading by example	0.0065
66	T25 -Empowerment Training	0.0065
67	T48 - Periodic review of public information	0.0059
68	T28 - Standardized computer platforms	0.0047
69	T30 - Recognition programs	0.0035

Section 5.2.1 will discuss in more detail the top 10 highest ranked tasks by indicating the various issues that should be addressed via their creation and implementation. The various issues that should be addressed via the creation and implementation of the lower 59 ranked objectives can be found in Table E.1 in Appendix E. It should be noted that omitting a detailed discussion for the lower 59 objectives in this section in no way is attempting to convey that they are not important; only that after

a discussion of the top 10 is presented, the reader is capable of understanding what is required to implement the last 59 tasks by examining Table E.1 in Appendix E.

As shown in Table 5.2, the highest ranked and obviously most important value-driven task for maximizing IS security within MSI Corp was that of security awareness training (T1) with a total score of 0.3859. A perfect score would be 1.0 which would mean that a particular task would be capable of attaining every sub-objective in the value hierarchy to the fullest degree. Thus it can be said that security awareness training was shown to have attained the sub-objectives shown in Table 4.1 to a degree of 39%. Of course, given the diversity of issues associated with the value hierarchy, achieving a perfect score or even a score higher than 0.5 is highly unlikely. As shown in Table 5.2, scores ranged from 0.0035 to 0.3859 where higher scores usually resulted from a particular task impacting several sub-objectives.

As shown in Table 5.3, T1 impacted a total of four fundamental objectives (two technical and two organizational) and fourteen of their associated sub-objectives. That is, making users aware of the fundamental issues surrounding the various sub-objectives for access control, data integrity, individual work ethic and data privacy and their importance to IS security via personal training programs is a very crucial part in attainment of these sub-objectives. As shown in Table 5.3, an adequate security awareness training program for MSI Corp should consist of topics that cover the fourteen sub-objectives shown in Table 5.3 that includes: accountability, levels of user access, physical security, user access based on "need to know," management oversight of user access issues, minimizing the temptation to use information for personal benefit, inappropriate changes to data, data

integrity controls, management oversight of data integrity issues, data privacy, disclosure awareness, and repercussions of sensitive data disclosure.

Table 5.3: Security Awareness Training

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
4. Maximize Access Control	4.1 Maintain personal accountability for system use	0.7	0.0378
	4.2 Ensure appropriate levels of user access	0.7	0.0517
	4.3 Ensure appropriate physical security	0.5	0.0560
	4.4 Ensure user access is based on "need to know"	0.7	0.0517
	4.5 Ensure adequate management oversight of access control	0.7	0.0378
5. Promote Individual Work Ethic	5.4 Minimize temptation to use information for personal benefit	0.7	0.0195
6. Maximize Data Integrity	6.1 Minimize inappropriate changes to data	0.7	0.1031
	6.2 Ensure appropriate data integrity controls for the processing of data	0.5	0.0883
	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.0736
8. Maximize Privacy	8.1 Emphasize importance of data privacy	0.7	0.013
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0142
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0134
	8.4 Ensure that sensitive data is adequately secured	0.5	0.0288
	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0118

As shown in Table 5.2, the second highest ranked task for maximizing IS security within MSI Corp was that of providing amendments to their already existing Guiding Principles (T21). As shown in Table 5.4, this task impacted a total of six organizational objectives and eighteen of their associated sub-objectives.

To implement this task, the Team indicated that MSI Corp's Guiding Principles should contain information that covers the fundamental issues surrounding IT competence, employee development and management practices, providing an ethical

environment, promoting individual work ethic, privacy and organizational integrity. Specifically, amendments to MSI Corp's Guiding Principles should cover the eighteen sub-objectives shown in Table 5.4 that includes: management teams leading by example, promoting contribution, instilling high levels of morale, creating pride, maintaining a motivated workforce, reporting unethical behavior, instilling professional-based work ethics, promoting organizational loyalty, employee integrity, sustaining the reputation of the company, promoting the organization's best interests rather than personal gain, minimizing the temptation to use information for personal benefit, data privacy, disclosure awareness, repercussions of sensitive data disclosure, empowerment, respect, and individual reliability. And as shown in Figure 4.1, some of these issues, such as respect and employee integrity, are already covered via MSI Corp's existing Guiding Principles.

Table 5.4: Amendments to Guiding Principles

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
1. Maximize IT Competence	1.1 Develop a management team that leads by example	0.5	0.0094
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution	0.5	0.0149
	2.2 Instill high levels of morale	0.7	0.0149
	2.3 Increase/maintain pride in the organization	0.7	0.0149
	2.4 Develop and maintain a motivated workforce	0.5	0.0149
3. Develop and Sustain an Ethical Environment	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.5	0.0161
	3.2 Instill professional-based work ethics	0.7	0.0265
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0121
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company	0.5	0.0325
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195
8. Maximize Privacy	8.1 Emphasize importance of data privacy	0.5	0.013
	8.2 Ensure employee awareness against disclosure of sensitive data	0.5	0.0142
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.5	0.0134
9. Maximize Organizational Integrity	9.1 Create an environment that empowers employees	0.5	0.0155
	9.2 Create an environment that promotes respect	0.7	0.0155
	9.3 Create an environment that promotes individual reliability	0.3	0.0155

As shown in Table 5.2, the third highest ranked task for maximizing IS security within MSI Corp was that of creating adequate authorization procedures (T5). As shown in Table 5.5, this task impacted a total of four fundamental objectives (two technical and two organizational) and four of their associated sub-objectives. To implement this task, the Team indicated that adequate authorization procedures should cover the fundamental issues surrounding access control, promoting individual work ethic, data integrity, and

privacy. Specifically, authorization procedures should be created that covers the four sub-objectives shown in Table 5.5 that includes: ensuring appropriate levels of user access, minimizing the temptation to use information for personal benefit, minimizing inappropriate changes to data, and ensuring that sensitive data is adequately secured.

Table 5.5: Authorization Procedures

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
4. Maximize Access Control	4.2 Ensure appropriate levels of user access	0.7	0.0517
5. Promote Individual Work Ethic	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195
6. Maximize Data Integrity	6.1 Minimize inappropriate changes to data	0.7	0.1031
8. Maximize Privacy	8.4 Ensure that sensitive data is adequately secured	0.7	0.0288

As shown in Table 5.2, the fourth highest ranked task for maximizing IS security within MSI Corp was that of creating and making known predefined roles and rights (T4) of the various system users within the organization. As shown in Table 5.6, this task impacted a total of three fundamental objectives (two technical and one organizational) and four of their associated sub-objectives. To implement this task, the Team indicated that adequate authorization procedures should cover the fundamental issues surrounding access control, data integrity, and privacy. Specifically, adequate predefined roles and rights should be created that cover the four sub-objectives shown in Table 5.6 that includes: ensuring appropriate levels of user access, ensuring user access is based on

"need to know," minimizing inappropriate changes to data, and ensuring that sensitive data is adequately secured.

Table 5.6: Pre-Defined Roles and Rights

Fundamental Objective	Impacts Sub-objective	Score	Global Weight
4. Maximize Access Control	4.2 Ensure appropriate levels of user access	0.7	0.0517
	4.4 Ensure user access is based on "need to know"	0.5	0.0517
6. Maximize Data Integrity	6.1 Minimize inappropriate changes to data	0.5	0.1031
8. Maximize Privacy	8.4 Ensure that sensitive data is adequately secured	0.5	0.0288

As shown in Table 5.2, the fifth highest ranked task for maximizing IS security within MSI Corp was that of providing amendments to their already existing Code of Business Conduct and Ethics (T22). As shown in Table 5.7, this task impacted a total of five organizational objectives and twelve of their associated sub-objectives. To implement this task, the Team indicated that MSI Corp's Code of Business Conduct and Ethics should contain information that covers the fundamental issues surrounding IT competence, providing an ethical environment, promoting individual work ethic, privacy, and organizational integrity. Specifically, amendments to MSI Corp's Code of Business Conduct and Ethics should cover the twelve sub-objectives shown in Table 5.7 that includes: management teams leading by example, reporting unethical behavior, instilling professional-based work ethics, employee integrity, sustaining the reputation of the company, promoting the organization's best interests rather than personal gain,

minimizing the temptation to use information for personal benefit, data privacy, disclosure awareness, repercussions of sensitive data disclosure, respect, and individual reliability.

Table 5.7: Amendments to Code of Business Conduct and Ethics

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
1. Maximize IT Competence	1.1 Develop a management team that leads by example	0.7	0.0094
3. Develop and Sustain an Ethical Environment	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.6	0.0161
	3.2 Instill professional-based work ethics	0.5	0.0265
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company	0.5	0.0325
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195
8. Maximize Privacy	8.1 Emphasize importance of data privacy	0.7	0.013
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0142
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0134
9. Maximize Organizational Integrity	9.2 Create an environment that promotes respect	0.7	0.0155
	9.3 Create an environment that promotes individual reliability	0.3	0.0155

As shown in Table 5.2, the sixth highest ranked task for maximizing IS security within MSI Corp was that of providing compensation and incentives that are tied to performance (T51). As shown in Table 5.8, appropriately implementing this task would

impact a total of four organizational objectives and eleven of their associated sub-objectives. To implement this task, the Team indicated that MSI Corp would be required to undertake a periodic and complete review of the organization's current compensation and incentives program to determine if they are truly tied to employee performance. Additionally, the Team felt that MSI Corp currently did a very god job of implementing this task thus only minimal changes would probably be required.

Table 5.8: Compensation and Incentives Tied to Performance

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution	0.9	0.0149
	2.2 Instill high levels of morale	0.8	0.0149
	2.3 Increase/maintain pride in the organization	0.7	0.0149
	2.4 Develop and maintain a motivated workforce	0.5	0.0149
3. Develop and Sustain an Ethical Environment	3.3 Create an environment that promotes organizational loyalty	0.7	0.0121
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company	0.5	0.0325
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195
9. Maximize Organizational Integrity	9.1 Create an environment that empowers employees	0.7	0.0155
	9.3 Create an environment that promotes individual reliability	0.6	0.0155

As shown in Table 5.2, the seventh highest ranked task for maximizing IS security within MSI Corp was that of creating an automated access monitoring system

(T12) to ensure appropriate system usage and to keep logs on various user activities. As shown in Table 5.9, implementing this task would impact a total of two technical objectives and two of their associated sub-objectives. To implement this task, the Team indicated that an adequate automated access monitoring system should, at the very least, cover the fundamental issues surrounding access control and data integrity. Specifically, an automated access monitoring system should be created that covers the two sub-objectives shown in Table 5.9 that includes: ensuring user access is based on "need to know," and minimizing inappropriate changes to data.

Table 5.9: Automated Access Monitoring System

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
4. Maximize Access Control	4.4 Ensure user access is based on "need to know"	0.7	0.0517
6. Maximize Data Integrity	6.1 Minimize inappropriate changes to data	0.7	0.1031

As shown in Table 5.2, the eighth highest ranked task for maximizing IS security within MSI Corp was that of providing a rewards program tied to employee performance (T52). As shown in Table 5.10, appropriately implementing this task would impact a total of four organizational objectives and nine of their associated sub-objectives. To implement this task, the Team indicated that MSI Corp would be required to undertake a periodic and complete review of the organization's current rewards program to determine if it is truly tied to employee performance and to determine if new rewards should be

considered. Additionally, as was the case with MSI Corp's compensation and incentives program, the Team felt that the organization currently did a very god job of implementing this task thus only minimal changes would be required.

Table 5.10: Rewards Program Tied to Employee Performance

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution	0.7	0.0149
	2.2 Instill high levels of morale	0.8	0.0149
	2.3 Increase/maintain pride in the organization	0.7	0.0149
	2.4 Develop and maintain a motivated workforce	0.9	0.0149
3. Develop and Sustain an Ethical Environment	3.3 Create an environment that promotes organizational loyalty	0.7	0.0121
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company	0.7	0.0325
	5.2 Create a desire to not jeopardize the reputation of the company	0.7	0.013
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.8	0.013
9. Maximize Organizational Integrity	9.3 Create an environment that promotes individual reliability	0.7	0.0155

As shown in Table 5.2, the ninth highest ranked task for maximizing IS security within MSI Corp was that of providing training and development programs for career advancement (T57). As shown in Table 5.11, appropriately implementing this task would impact a total of four organizational objectives and ten of their associated sub-objectives. To implement this task, the Team indicated that MSI Corp would be required to periodically undertake a complete review of the organization's current training and development programs for career advancement to determine if any new programs would be required. As shown in Table 5.11, solid training and development programs for career

advancement would impact issues that include: creating an environment that promotes contribution, instilling high levels of morale, increasing pride, developing a motivated workforce, creating an environment that promotes organizational loyalty, maximizing employee integrity, promoting the organization's best interests rather than personal gain, minimizing the temptation to use information for personal benefit, and creating an environment that promotes both empowerment and individual reliability.

Table 5.11: Provide Training and Development Programs for Career Advancement

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution	0.5	0.0149
	2.2 Instill high levels of morale	0.6	0.0149
	2.3 Increase/maintain pride in the organization	0.6	0.0149
	2.4 Develop and maintain a motivated workforce	0.8	0.0149
3. Develop and Sustain an Ethical Environment	3.3 Create an environment that promotes organizational loyalty	0.7	0.0121
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company	0.8	0.0325
	5.2 Create a desire to not jeopardize the reputation of the company	0.3	0.013
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.5	0.013
9. Maximize Organizational Integrity	9.1 Create an environment that empowers employees	0.8	0.0155
	9.3 Create an environment that promotes individual reliability	0.8	0.0155

And finally, as shown in Table 5.2, the tenth highest ranked task for maximizing IS security within MSI Corp was that of providing an adequate contribution/matching program (T55). As shown in Table 5.12, appropriately implementing this task would impact a total of four organizational objectives and ten of their associated sub-objectives.

To implement this task, the Team indicated that MSI Corp would be required to periodically undertake a complete review of the organization's current contribution/matching program to determine if any new additions would be required. As shown in Table 5.12, adequate implementation of this task would impact issues that include: creating an environment that promotes contribution, increasing pride, developing a motivated workforce, creating an environment that promotes organizational loyalty, maximizing employee integrity, promoting the organization's best interests rather than personal gain, minimizing the temptation to use information for personal benefit, and creating an environment that promotes individual reliability.

Table 5.12: Contribution/Matching Program

Fundamental Objective	Impacts Sub-Objective	Score	Global Weight
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution	0.7	0.0149
	2.2 Instill high levels of morale	0.7	0.0149
	2.3 Increase/maintain pride in the organization	0.7	0.0149
	2.4 Develop and maintain a motivated workforce	0.8	0.0149
3. Develop and Sustain an Ethical Environment	3.3 Create an environment that promotes organizational loyalty	0.5	0.0121
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company	0.5	0.0325
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.0130
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.0130
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195
9. Maximize Organizational Integrity	9.3 Create an environment that promotes individual reliability	0.7	0.0155

5.3 Sensitivity Analysis

Table 5.2 provides a comprehensive and ranked list of value-driven alternatives that are required for maximizing IS security within MSI Corp. The final rankings shown in Table 5.2 were generated via Equation 1 which relies on the weights that were determined using the swing weighting method discussed in Section 4.5. Because the swing weighting method or any weighting technique is somewhat subjective, sensitivity analysis is recommended as it examines the validity of the findings by removing the subjective nature of the weights and can often times provide the DM with valuable insight.

To accomplish this analysis, the weight of each value is systematically altered and the subsequent impact on the final task scores and rankings are tracked. As an individual weight is changed, the other weights are adjusted to ensure that the sum of the column or section remains 1.0. And the proportionality of the other weights to each other is maintained as the weight being assessed is adjusted.

Because three natural categories existed for this research that consisted of technical, socio-technical and social objectives, it was determined that 100% weight would be given to each of these three categories to determine a ranking of the various tasks in isolation for each of these three categories. This type of analysis provides MSI Corp with a better understanding of the specific tasks that relate to the individual categories.

5.3.1 100% Technical

Table 5.13 indicates the adjusted global weights of the technical objectives when 100% weight was given to this category. As shown in Table 4.14 in Section 4.4, the technical category was initially given 50% weight. Thus the actual global weights for the technical objectives simply need to be multiplied by 2 and as shown in Table 5.13, the sum of these global weights then becomes 1.0.

Table 5.13: Adjusted Global Weights for 100% Technical

Fundamental Objective	Local Weight	Sub-Objective	Local Weight	Actual Global Weight	Adjusted Global Weight
4. Maximize Access Control	**0.47**	**4.1**	0.161	0.038	**0.076**
		4.2	0.220	0.052	**0.103**
		4.3	0.238	0.056	**0.112**
		4.4	0.220	0.052	**0.103**
		4.5	0.161	0.038	**0.076**
6. Maximize Data Integrity	**0.53**	**6.1**	0.389	0.103	**0.206**
		6.2	0.333	0.088	**0.177**
		6.3	0.278	0.074	**0.147**
					Total = 1.0

Table 5.14 then illustrates the rankings of the technical tasks when 100% weight was given to the technical category. The actual calculations to derive Table 5.14 are shown in Appendix E. As shown in Table 5.14, the rank ordering changed slightly. For example, T5 moved from second position down to the third position and was shown to be equivalent to T12. These slight changes in rank were as a result of removing the impacts that any of these tasks had on the organizational objectives. In other words, T5 obviously impacted the organizational objectives to a higher degree than T4 thus when removing

these impacts, T4 moved up in rank when considering the technical objectives alone. Additionally, as shown in Table 5.14, security awareness training attained the technical sub-objectives to a degree of approximately 67% which provides further quantitative evidence of its importance for maximizing IS security within MSI Corp.

Table 5.14: Adjusted Task Rankings (100% Technical)

Rank	Actual Rank	Task	Final Score $\Sigma w_i * v_i(x_i)$
1	1	T1 – Security Awareness Training	0.6696
2	4	T4 – Pre-defined roles and rights	0.2272
3	3	T5 - Authorization procedures	0.2167
4	7	T12 - Automated access monitoring system	0.2167
5	14	T14 – Security administration group/policy makers	0.1560
6	16	T10 - Well-defined job descriptions	0.1548
7	17	T11 – Segregation of duties matrix	0.1548
8	18	T17 - Edit and validation routines	0.1413
9	20	T18 – Reconciliation procedures	0.1236
10	25	T19 – Periodic error log audits	0.1030
11	26	T20 – Periodic review of reconciliations	0.1030
12	21	T7 – Badges/key cards	0.0784
13	22	T9 - Security guards	0.0784
14	24	T2 - Limit the use of group accounts or generic IDs	0.0688
15	28	T8 - Video surveillance	0.0560
16	29	T3 – Password controls to force unique logons	0.0529
17	38	T13 – Periodic review of user access roles and rights	0.0529
18	27	T6- Centralized system administration	0.0517
19	45	T15 – Audit log reviews	0.0378
20	46	T16 - Review of termination lists (centralized review)	0.0378

5.3.2 100% Socio-Technical

Table 5.15 indicates the adjusted global weights of the socio-technical objectives when 100% weight was given to this category. As shown in Table 4.14 in Section 4.4,

the socio-technical category was a subset of the organizational category and was initially given 45% weight. Thus to obtain the adjusted global weights, the organizational and socio-technical categories were moved to 100% from 50% and 45%, respectively. In other words, the actual weights shown in Table 5.15 were divided by 0.50 and 0.45 to obtain the adjusted global weights.

Table 5.15: Adjusted Global Weights for 100% Socio-Technical

Fundamental Objective	Local Weight	Sub-objective	Local Weight	Actual Global Weight	Adjusted Global Weight
1. Maximize IT Competence	**0.299**	**1.1**	0.140	0.009	**0.042**
		1.2	0.140	0.009	**0.042**
		1.3	0.175	0.012	**0.052**
		1.4	0.228	0.015	**0.068**
		1.5	0.317	0.021	**0.095**
7. Enhance Integrity of Business Processes	**0.34**	**7.1**	0.347	0.027	**0.118**
		7.2	0.191	0.015	**0.065**
		7.3	0.462	0.035	**0.157**
8. Maximize Privacy	**0.361**	**8.1**	0.160	0.013	**0.058**
		8.2	0.175	0.014	**0.063**
		8.3	0.165	0.013	**0.060**
		8.4	0.354	0.029	**0.128**
		8.5	0.146	0.012	**0.053**
					Total = 1.0

Table 5.16 then illustrates the rankings of the socio-technical tasks when 100% weight was given to the socio-technical category. The actual calculations to derive Table 5.16 are shown in Appendix E. As shown in Table 5.16, a number of tasks that were not ranked in the overall top 10 had a major impact when considering the socio-technical objectives alone. For example, process design training (T35) which had an actual ranking of 13 was ranked first when giving 100% weight to the socio-technical category.

In fact, as shown in Table 5.16, process design training attained the socio-technical sub-objectives to a degree of approximately 38% which provides quantitative evidence that it should not be overlooked. Other tasks that had lower actual ranks that should be heavily considered as a result of this sensitivity analysis include: documenting and making known business processes (T36), creating and making known information classification standards (T37), and IT training and development (T26).

Table 5.16: Adjusted Task Rankings (100% Socio-Technical)

Rank	Actual Rank	Task	Final Score
1	13	T35 - Process design training	0.3845
2	1	T1 – Security Awareness Training	0.2270
3	31	T36 - Document and make known business processes	0.1636
4	32	T37 -Create and make known information classification standards	0.1636
5	5	T22 - Amendments to Code of Business Conduct and Ethics	0.1556
6	33	T26 - IT Training and development	0.1431
7	35	T43 - Amendments to Employee Manual	0.1263
8	39	T33 - Individual development plans	0.1139
9	2	T21- Amendments to Guiding Principles	0.1111
10	40	T40 - Risk assessment activities	0.1101
11	41	T41 - Periodic review of business process improvement program	0.1101
12	42	T42 -Executive management oversight	0.1101
13	43	T32 - Skills assessments and performance evaluations	0.1097
14	27	T6- Centralized system administration	0.1024
15	44	T44 - Posters in the coffee room	0.0902
16	24	T2 - Limit the use of group accounts or generic IDs	0.0896
17	29	T3 - Password controls to force unique logons	0.0896
18	3	T5 - Authorization procedures	0.0896
19	21	T7 – Badges/key cards	0.0896
20	28	T8 – Video surveillance	0.0896
21	22	T9 - Security guards	0.0896
22	48	T27 – Hire employees with adequate IT skills	0.0682
23	4	T4 - Pre-defined roles and rights	0.0640
24	23	T45 – Nondisclosure agreement with repercussions	0.0568
25	54	T34 - Budget for Training	0.0476

5.3.3 100% Social

Table 5.17 indicates the adjusted global weights of the social objectives when 100% weight was given to this category. As shown in Table 4.14 in Section 4.4, the social category was a subset of the organizational category and was initially given 55% weight. Thus to obtain the adjusted global weights, the organizational and social categories were moved to 100% from 50% and 55%, respectively. In other words, the actual weights shown in Table 5.17 were divided by 0.50 and 0.55 to obtain the adjusted global weights.

Table 5.17: Adjusted Global Weights for 100% Social

Fundamental Objective	Local Weight	Sub-Objective	Local Weight	Actual Global Weight	Adjusted Global Weight
2. Promote Employee Development and Management Practices	**0.216**	**2.1**	0.250	0.015	**0.054**
		2.2	0.250	0.015	**0.054**
		2.3	0.250	0.015	**0.054**
		2.4	0.250	0.015	**0.054**
3. Develop and Sustain an Ethical Environment	**0.284**	**3.1**	0.206	0.016	**0.058**
		3.2	0.339	0.026	**0.096**
		3.3	0.156	0.012	**0.044**
		3.4	0.300	0.023	**0.085**
5. Promote Individual Work Ethic	**0.284**	**5.1**	0.417	0.033	**0.118**
		5.2	0.167	0.013	**0.047**
		5.3	0.167	0.013	**0.047**
		5.4	0.250	0.020	**0.071**
9. Maximize Organizational Integrity	**0.216**	**9.1**	0.261	0.016	**0.056**
		9.2	0.261	0.016	**0.056**
		9.3	0.261	0.016	**0.056**
		9.4	0.216	0.013	**0.047**
					Total = 1

Table 5.18 then illustrates the rankings of the social tasks when 100% weight was given to the social category. The actual calculations to derive Table 5.18 are shown in Appendix E. As shown in Table 5.18, as was the case with the technical objectives, the rank ordering only changed slightly when giving 100% weight to the social category. For example, T22 moved from an actual rank of fifth to a rank of ninth. These slight changes in rank were as a result of removing the impacts that any of these tasks had on the socio-technical objectives. In other words, T22 obviously impacted the socio-technical objectives to a higher degree than many of the other tasks shown in Table 4.13. Additionally, as shown in Table 5.14, creating amendments to MSI Corp's Guiding Principles attained the social sub-objectives to a degree of approximately 48% which provides further quantitative evidence of its importance for maximizing IS security within MSI Corp. Table 5.18 also brings attention to the importance of authority delegation (T50), having well-defined career paths (T53), open communication policies (T54), and teambuilding exercises (T56), as they all scored greater than 0.20 when isolating the social objectives.

Table 5.18: Adjusted Task Rankings (100% Social)

Rank	Actual Rank	Task	Final Score
1	2	T21- Amendments to Guiding Principles	0.4846
2	6	T51 - Compensation and incentives tied to performance	0.4125
3	8	T52 - Rewards program	0.3919
4	9	T57 - Provide training and development programs for career advancement	0.3888
5	10	T55 - Contribution/matching program	0.3699
6	11	T50 - Authority delegation (written document for empowerment)	0.3575
7	12	T53 – Well-defined career paths	0.3179
8	15	T54 - Open communication policy	0.3060
9	5	T22 - Amendments to Code of Business Conduct and Ethics	0.2909
10	19	T56 - Teambuilding Exercises	0.2349
11	30	T61 - Chief Ethics Officer	0.1355
12	23	T45 – Nondisclosure agreement with repercussions	0.1158
13	34	T62 - Ethics Committee	0.1053
14	36	T63 - Ethics officer reports to the board or audit committee	0.0968
15	37	T64 - Periodic ethics questionnaires of employees	0.0968
16	47	T65 - Employees reaffirm (written test) ethics policy on a periodic basis	0.0596
17	49	T58 – Ethics Hotline	0.0527
18	50	T66 - Performance management including upward feedback	0.0451
19	51	T67 - Performance evaluations	0.0451
20	52	T60 - Hiring policies (background and credit checks)	0.0419
21	53	T59 - Policy of no retaliation to employees who report suspected issues	0.0410
22	55	T69 - Board and Audit Committee periodic review of business plans	0.0372
23	59	T68 - Budget/Financial reviews	0.0326

5.4 Recommendations

Table 5.19 provides a ranked listing along with recommended actions for each of the 69 value-driven tasks. Additionally, Table 5.19 provides information in terms of whether or not MSI Corp is currently implementing the various tasks and any initial and future costs associated with reviewing, updating or implementing the various tasks. As shown in Table 5.19, the 'Existing' column consists of three possible values that include: 'No,' 'Somewhat,' and 'Yes.' And the 'Additional Cost' columns consist of five possible values that include: 'Minimal,' 'Low,' 'Medium,' 'Moderate,' and 'High.' These values were obtained via one additional interview with the Team after the final rankings were determined.

Table 5.19: Task Rankings with Additional Costs and Recommended Actions

Rank	Task	Final Score	Existing?	Additional Cost		Proposed Action
				Initial	Future	
1	T1 – Security Awareness Training	0.386	Somewhat	Medium	Low	Update
2	T21- Amendments to Guiding Principles	0.158	Somewhat	Minimal	Minimal	Update
3	T5 – Authorization procedures	0.138	Yes	Minimal	Minimal	Review
4	T4 – Pre-defined roles and rights	0.128	Somewhat	Minimal	Minimal	Update
5	T22 - Amendments to Code of Business Conduct and Ethics	0.115	Somewhat	Minimal	Minimal	Update
6	T51 - Compensation and incentives tied to performance	0.113	Yes	Minimal	Minimal	Review
7	T12 - Automated access monitoring system	0.108	Somewhat	Medium	Low	Update
8	T52 - Rewards program tied to employee performance	0.108	Yes	Minimal	Minimal	Review

9	T57 - Provide training and development programs for career advancement	0.107	Somewhat	Medium	Low	Update
10	T55 - Contribution/matching program	0.102	Yes	Minimal	Minimal	Review
11	T50 - Authority delegation (written document for empowerment)	0.098	Yes	Minimal	Minimal	Review
12	**T53 – Well-defined career paths**	0.087	**No**	Low	Low	**Implement**
13	**T35 - Process design training**	0.087	**No**	Medium	Low	**Investigate**
14	T14 - Security administration group/policy makers	0.086	Yes	Low	Low	Review
15	T54 - Open communication policy	0.084	Somewhat	Minimal	Minimal	Review
16	T10 – Well-defined job descriptions	0.077	Yes	Minimal	Minimal	Review
17	T11 – Segregation of duties matrix	0.077	Somewhat	Minimal	Minimal	Update
18	T17 – Edit and validation routines	0.071	Somewhat	Minimal	Minimal	Update
19	T56 – Teambuilding Exercises	0.065	Somewhat	Minimal	Minimal	Update
20	T18 – Reconciliation procedures	0.062	Yes	Low	Low	Review
21	T7 – Badges/key cards	0.059	Yes	Minimal	Minimal	Review
22	T9 – Security guards	0.059	Yes	Minimal	Minimal	Review
23	T45 – Nondisclosure agreement with repercussions	0.057	Somewhat	Minimal	Minimal	Update
24	T2 – Limit the use of group accounts or generic IDs	0.055	Somewhat	Minimal	Minimal	Update
25	T19 – Periodic error log audits	0.052	Somewhat	Low	Low	Update
26	T20 – Periodic review of reconciliations	0.052	Somewhat	Low	Low	Update
27	T6- Centralized system administration	0.049	Somewhat	Medium	Medium	Update
28	T8 – Video surveillance	0.048	Yes	Minimal	Minimal	Review
29	T3 - Password controls to force unique logons	0.047	Yes	Minimal	Minimal	Review
30	T61 - Chief Ethics Officer	0.037	Yes	Minimal	Minimal	Review
31	T36 – Document and make known business processes	0.037	Somewhat	Low	Low	Update
32	**T37 -Create and make known information classification standards**	0.037	**No**	Low	Minimal	**Implement**

33	T26 - IT Training and development	0.032	Somewhat	Moderate	Low	Update
34	T62 - Ethics Committee	0.029	Yes	Low	Low	Review
35	T43 - Amendments to Employee Manual	0.028	Somewhat	Minimal	Minimal	Update
36	T63 - Ethics officer reports to the board or audit committee	0.027	Yes	Minimal	Minimal	Review
37	T64 - Periodic ethics questionnaires of employees	0.027	Yes	Minimal	Minimal	Review
38	T13 - Periodic review of user access roles and rights	0.027	Yes	Low	Low	Review
39	T33 – Individual development plans	0.026	Yes	Minimal	Minimal	Review
40	T40 – Risk assessment activities	0.025	Somewhat	Low	Low	Update
41	**T41 - Periodic review of business process improvement program**	0.025	**No**	Low	Low	**Implement**
42	T42 -Executive management oversight	0.025	Yes	Minimal	Minimal	Review
43	T32 - Skills assessments and performance evaluations	0.025	Yes	Minimal	Minimal	Review
44	T44 – Posters in the coffee room	0.020	Somewhat	Minimal	Minimal	Update
45	T15 – Audit log reviews	0.019	Yes	Minimal	Minimal	Review
46	T16 – Review of termination lists (centralized review)	0.019	Yes	Minimal	Minimal	Review
47	T65 - Employees reaffirm (written test) ethics policy on a periodic basis	0.016	Yes	Minimal	Minimal	Review
48	T27 – Hire employees with adequate IT skills	0.015	Somewhat	Low	Low	Update
49	T58 – Ethics Hotline	0.015	Yes	Minimal	Minimal	Review
50	T66 – Performance management including upward feedback	0.012	Yes	Minimal	Minimal	Review
51	T67 – Performance evaluations	0.012	Yes	Minimal	Minimal	Review
52	T60 - Hiring policies (background and credit checks)	0.012	Yes	Minimal	Minimal	Review
53	T59 - Policy of no retaliation to employees who report suspected issues	0.011	Yes	Minimal	Minimal	Review
54	T34 – Budget for training	0.011	Somewhat	Medium	Medium	Update
55	T69 - Board and Audit Committee periodic review of business plans	0.010	Yes	Minimal	Minimal	Review

56	T38 - Create and manage a business process improvement program	0.010	Somewhat	Medium	Low	Update
57	T39 - Create and adhere to business process maturity/lifecycle model	0.010	Somewhat	Minimal	Minimal	Update
58	T29 – Compensation programs aligned with company values	0.009	Yes	Minimal	Minimal	Review
59	T68 – Budget/Financial reviews	0.009	Yes	Minimal	Minimal	Review
60	T31 - Goals and incentives tied to job descriptions and performance	0.008	Yes	Minimal	Minimal	Review
61	T46 – Privacy officer	0.008	Yes	Minimal	Minimal	Review
62	T47 - Incident response team	0.008	Somewhat	Low	Low	Update
63	T49 - Oversee privacy aspects of Security Awareness Training	0.008	Somewhat	Minimal	Minimal	Update
64	T23 – Written in Job Descriptions	0.007	Yes	Minimal	Minimal	Review
65	T24 - Compensation/ incentive programs designed to influence management teams leading by example	0.007	Yes	Minimal	Minimal	Review
66	T25 –Empowerment Training	0.007	Somewhat	Low	Low	Update
67	T48 - Periodic review of public information	0.006	Somewhat	Low	Low	Update
68	T28 – Standardized computer platforms	0.005	Somewhat	Moderate	Low	Update
69	T30 – Recognition programs	0.004	Yes	Minimal	Minimal	Review

- **Cost Values (Minimal, Low, Medium, Moderate, High)**
- **Existing Values (No, Somewhat, Yes)**
- **Recommended Action**
  - **Implement = A new task that should be implemented by MSI Corp**
  - **Investigate = A new task that requires further analysis before implementing**
  - **Update = A somewhat existing task that needs to be updated to at least match the sub-objectives it impacts as shown in Table E.1 in Appendix E**
  - **Review = A tasks that the Team indicated is currently being implemented to its highest degree; however, a periodic review should be conducted to verify this task's impact on its related sub-objectives as shown in Table E.1 in Appendix E**

5.4.1 Implementing New Tasks

As shown in Table 5.19, only four of the 69 value-driven tasks are not currently being implemented in some form at MSI Corp. These tasks include: establishing well-defined career paths (T53), providing process design training (T35), creating and making known information classification standards (T37), and conducting a periodic review of MSI Corp's existing business process improvement program (T41).

As shown in Table 5.19, T53 was ranked rather high (12^{th}) in comparison to the other value-driven tasks and was shown to attain the sub-objectives of the entire value hierarchy to a degree of approximately 9%. And as shown in Table 5.17 in Section 5.3.3, when 100% weight was given to the social category, T53 was ranked 7^{th} out of 23 and was shown to attain the social sub-objectives alone to a degree of approximately 32%. Additionally, the costs associated with implementing this task, both in terms of initial and future costs were shown to be low.

Thus it is recommended that MSI Corp take actions to create and make known the various career paths that are available within the organization. As shown in Table E.1 in Appendix E, creating and making known well-defined career paths will positively impact a total of ten sub-objectives that includes: creating an environment that promotes contribution, instilling high levels of morale, increasing/maintaining pride in the organization, developing and maintaining a motivated workforce, creating an environment that promotes organizational loyalty, maximizing employee integrity in the company, creating a desire to not jeopardize the reputation of the company, creating an environment that promotes the organization's best interests rather than personal gain,

creating an environment that empowers employees, and creating an environment that promotes individual reliability.

As shown in Table 5.19, T35 was ranked rather high in comparison to the other value-driven tasks and was shown to attain the sub-objectives of the entire value hierarchy to a degree of approximately 9% as well. And as shown in Table 5.16 in Section 5.3.2, when 100% weight was given to the socio-technical category, T35 was ranked 1st out of 39 and was shown to attain the socio-technical sub-objectives alone to a degree of approximately 38%. However, the initial cost associated with implementing this task was shown to be higher than the other tasks which may cause some concern for MSI Corp.

Thus it is recommended that MSI Corp investigates creating business process design training for its employees with further analysis outside the scope of this research. As shown in Table E.1 in Appendix E, creating business process design training for MSI Corp's employees will positively impact a total of three sub-objectives that includes: understanding the expected use of available information and its relation to individual business processes, ensuring that appropriate organizational controls are in place, and developing procedures for managing changes to business processes.

As shown in Table 5.19, T37 was ranked in the middle in comparison to the other value-driven tasks and was shown to attain the sub-objectives of the entire value hierarchy to a degree of approximately 4%. Additionally, the costs associated with implementing this task, both in terms of initial and future costs, were shown to be low.

Thus it is recommended that MSI Corp take actions to create and make known information classification standards within the organization. As shown in Table E.1 in Appendix E, creating and making known information classification standards will positively impact sub-objective 7.1, "understand the expected use of available information and its relation to individual business processes."

And finally, as shown in Table 5.19, T41 was ranked in the middle in comparison to the other value-driven tasks and was shown to attain the sub-objectives of the entire value hierarchy to a degree of approximately 3%. Additionally, the costs associated with implementing this task, both in terms of initial and future costs, were shown to be low as well.

Thus it is recommended that MSI Corp take actions to conduct a periodic review of its existing business process improvement program. As shown in Table E.1 in Appendix E, conducting a periodic review of MSI Corp's existing business process improvement program will positively impact sub-objective 7.3, "ensure that appropriate organizational controls are in place."

5.4.2 Updating and Reviewing Existing Tasks

As shown in Table 5.19, the Team indicated that a total of 29 of the 69 value-driven tasks are currently 'somewhat' being implemented and a total of 36 of the 69 value-driven tasks are currently being implemented to their fullest degree ('yes') at MSI Corp. As shown in Table 5.19, values of 'somewhat' and 'yes' for the 'Existing' column led to the recommended actions of 'update' and 'review,' respectfully.

For example, in terms of updatin existing tasks, MSI Corp currently has a security awareness training program (T1). However, to obtain the sub-objectives that this research deemed this task should impact, MSI Corp's existing security awareness training program should focus on at least the issues that cover the fourteen sub-objectives shown in Table E.1 in Appendix E. These issues include: accountability, levels of user access, physical security, user access based on "need to know," management oversight of user access issues, minimizing the temptation to use information for personal benefit, inappropriate changes to data, data integrity controls, management oversight of data integrity issues, data privacy, disclosure awareness, and repercussions of sensitive data disclosure. Because the Team indicated that MSI Corp's current security awareness training program does not cover all of these issues, it is recommended that the organization updates this particular program to match these fourteen security issues shown in Table E.1 in Appendix E.

Furthermore, because additional costs associated with updating the other 28 value-driven tasks shown in Table 5.19 are rather low, it is recommended that similar logic be applied to these other 28 tasks. That is, for each of the 'somewhat' existing tasks in Table 5.19, MSI Corp should investigate the sub-objectives that they impact shown in Table E.1 in Appendix E and update each of these tasks accordingly.

In terms of reviewing existing tasks, MSI Corp, for example, currently implements authorization procedures (T5). As shown in Table E.1 in Appendix E, these procedures should be created in such a manner that they positively impact issues such as: minimizing the temptation to use information for personal benefit, minimizing

inappropriate changes to data, ensuring that sensitive data is adequately secured, and ensuring appropriate levels of user access. Because the Team indicated that they believe that current authorization procedures are written in a manner that at least account for these issues, it is recommended that a periodic review is conducted to determine the effectiveness of MSI Corp's current authorization procedures in the context of these issues.

Furthermore, because additional costs associated with reviewing the other 35 value-driven tasks shown in Table 5.19 are minimal, it is recommended that similar logic be applied to these other 35 tasks. That is, MSI Corp should periodically analyze each of the tasks in Table 5.19 with a recommended action of 'review,' via the sub-objectives that they impact shown in Table E.1 in Appendix E to determine the effectiveness of MSI Corp's current authorization procedures in the context of these issues.

Chapter 6 - Conclusions

6.1 Introduction

This dissertation created a decision model for maximizing IS security within an organization. The purpose of Chapter 6 is to bring together the key ideas that contributed to this dissertation. A summary of the key concepts and main contributions of this dissertation will be identified, along with the limitations of this research. Additionally, Chapter 6 will provide some directions for future research to extend the efforts of this work.

6.2 Summary of Key Concepts and Contributions

This research examined the current state of IS security and documented some shortcomings of traditional IS security practices such as checklists, risk management and formal methods. In short, due to the fact that these traditional techniques have been shown to concentrate solely on technical matters and the fact that they tend to rely on information that is already known, giving these techniques limited ability to deal with the dynamic and ever-changing world of IS security, a broader and more dynamic perspective that accounts for both technical and organizational issues was found to be more appropriate when considering IS security.

This research then examined Dhillon and Torkzadeh's (2006) existing theoretical framework of 9 fundamental and 16 means objectives for maximizing IS security in an

organization. These objectives were derived using a value-focused thinking approach and illustrate that both technical and socio-organizational issues are indeed valued by decision makers responsible for maintaining IS security. Dhillon and Torkzadeh's (2006) framework provides a rigorous theoretical base for considering IS security from the socio-organizational perspective; yet before the efforts of this research, no current methodology existed to assess these objectives so that informed decisions could be made in the context of maximizing IS security.

As a result, this research investigated and implemented a 10-step methodology in an effort to operationalize Dhillon and Torkzadeh's (2006) framework of 9 fundamental and 16 means objectives. This methodology was based on a value-focused thinking (VFT) approach and led to the creation of a decision model for maximizing IS security. This decision model was then used to provide insight to the organization studied in this research (MSI Corp) in terms of creating and selecting informed, value-driven tasks that relate to maximizing IS security within their organization. Additionally, because many tasks were in the form of periodic reviews via organizational management oversight functions, it can be said that the decision model created in this research is dynamic in nature and is capable of addressing future security concerns as they arise.

6.2.1 Main Contributions

The results of this research effort provide practical, methodological and theoretical contributions to the IS security literature stream and are as follows:

Practical: The results of this research are groundbreaking in that for the first time, both technical and organizational issues related to IS security were analyzed together to create a decision model for maximizing IS security within an organization. This decision model consisted of 69 value-driven tasks along with rankings (Table 5.2) and their various relationships (Table E.1, Appendix E) to the several security objectives that this research found were valued by MSI Corp. As a result of the analysis conducted in this research, valid recommendations were then made to MSI Corp in terms of what new tasks should be implemented and the actions that MSI Corp should take for already-existing tasks.

For MSI Corp, the value hierarchy, evaluation measures, value functions, weighting scheme, and ranked tasks created in this research will prove useful for aiding the decision making process in the context of enhancing IS security in their organization. And for other organizations, the results of this research effort provide a practical starting point for creating their own specific decision model. Undoubtedly, the lessons learned in this research will serve to minimize the time required to create similar decision models that relate to the specific values of other organizations for purposes of maximizing IS security.

Methodological: This research effort proved that both technical and organizational issues that relate to IS security can in fact be concurrently analyzed in an objective or quantifiable manner to assist in the decision making process for maximizing IS security. In other words, this research clearly demonstrates that the 10-step VFT process implemented in this research provides a feasible methodology for assisting

decision makers in creating and selecting appropriate value-driven tasks used for maximizing IS security within any organization.

Theoretical: This research provided two main theoretical contributions. First, via the creation of the amended fundamental hierarchy shown in Table 4.1, a new conceptualization of IS security emerged, as shown in Figure 6.1 below. And second, the results of this research provide for the first time theoretical relationships between 69 value-driven tasks and the associated security objectives that they impact.

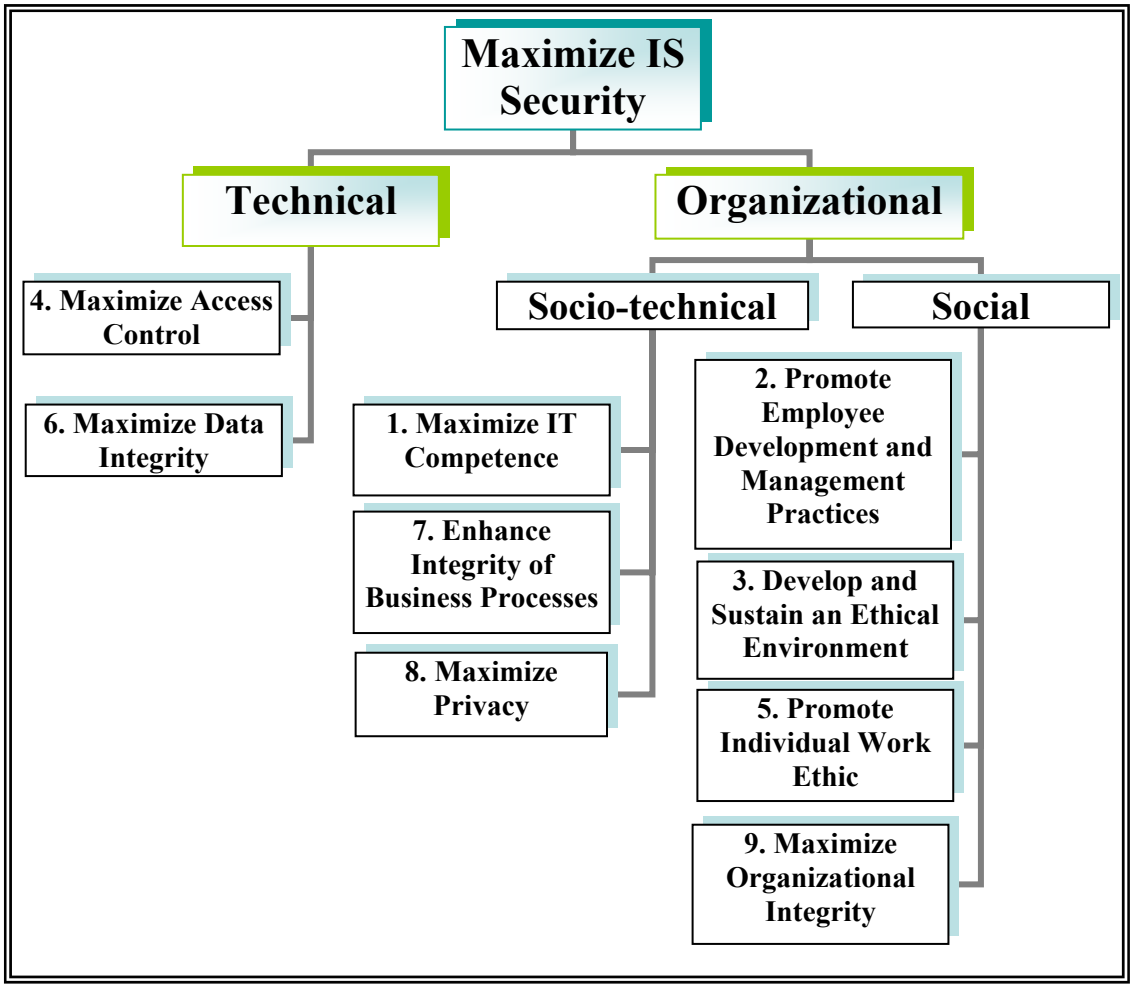

Figure 6.1: Conceptual Hierarchy for Maximizing IS Security

As shown in Figure 6.1, three categories for IS security emerged and consisted of technical, socio-technical, and social elements. The technical objectives shown in Figure 6.1 were defined as those that required technical expertise to implement and to monitor. That is, the issues of access control and data integrity requires a certain amount of technical expertise from both the IT department to implement and from various managers throughout the organization to monitor. Social objectives were then defined as those that required managerial and organizational expertise to implement and to monitor. For example, to "develop and sustain an ethical environment" does not require any technical expertise from the IT department. And socio-technical objectives were defined as those that required a combination of both technical and organizational expertise to implement and to monitor.

Figure 6.2 then illustrates one example of the many new relationships found in this research between the 69 value-driven tasks and the associated security issues that they impact. As shown in Figure 6.2, providing adequate compensation and incentive programs was shown in this research to impact issues that included: (2.1) creating an environment that promotes contribution, (2.2) instilling high levels of morale, (2.3) increasing and maintaining pride in the organization, (2.4) developing and maintaining a motivated workforce, (3.3) creating an environment that promotes organizational loyalty, (5.1) maximizing employee integrity in the company, (5.2) creating a desire to not jeopardize the reputation of the company, (5.3) creating an environment that promotes the organization's best interests rather than personal gain, (5.4) minimizing temptation to use information for personal benefit, (9.1) creating an environment that empowers employees,

and (9.3) creating an environment that promotes individual reliability. These issues then impact the more fundamental issues that include: (2) promoting employee development and management practices, (3) developing and sustaining an ethical environment, (5) promoting individual work ethic, and (9) maximizing organizational integrity. The remainder of these relationships can be derived from examining Table E.1 in Appendix E.

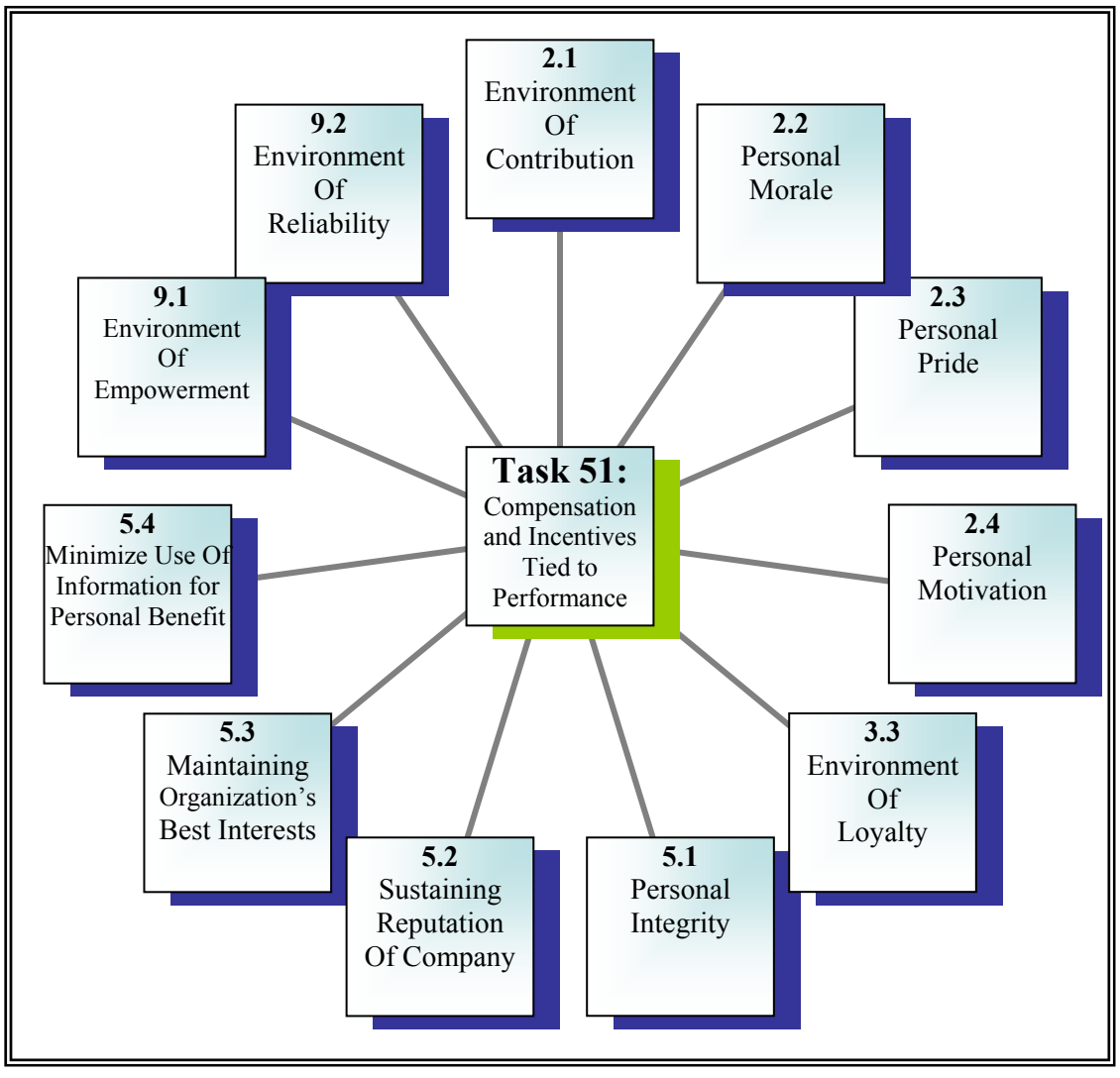

Figure 6.2: Security Issues that Task 51 "Compensation and Incentives" Impacts

6.3 Research Limitations

One limitation of this research is that uncertainty is only addressed through the sensitivity analysis performed on the weights assigned to the amended objective hierarchy shown in Table 4.1. However, this sensitivity analysis does not consider the uncertainty associated with the construction of the value functions nor the scores derived for the various tasks. Of course, special attention was given to arriving at a systematic consensus for the creation of the various value functions and the scores obtained for the various tasks; yet arriving at this consensus was still rather subjective. Therefore, uncertainty exists in the final rankings of the 69 value-driven tasks shown in Table 5.2 in Section 5.4. As was also shown in the recommendation section (Section 5.4) of this dissertation, these rankings were not heavily relied upon as all of the 69 value-driven tasks were given similar attention in terms of proposed actions shown in Table 5.2.

Another limitation of this research may be the fact that the research Team only consisted of three individuals from the organization. These three individuals were burdened with the job to identify and weight security objectives and discover and score tasks related to the values of the entire organization. It could be argued that these three individuals alone could not speak for all of the values of this very large organization and come up with a completely exhaustive list of security objectives and tasks. However, much of the burden to come up with an exhaustive list of security objectives was removed by using Dhillon and Torkzadeh's (2006) already-existing framework of 9 fundamental objectives and their associated sub-objectives as a template. Additionally, other researchers have noted using small numbers of employees to represent an

organization's values can in fact provide accurate research results. For example, Phythian and King (1992) used two manager experts to develop rules for an expert system to support customer tender evaluations; yet it should be noted that the 69 value-driven tasks found in this research may not be completely exhaustive.

A final limitation of this research is that only two technical objectives existed as compared to seven organizational objectives. Because both the technical and organizational categories were given equal weight, as shown in Table 4.14 in Section 4.4, it naturally followed that the global weights for the technical objectives would be much higher than that of the global weights of the organizational objectives. However, because final rankings were a function of both global weight and the number of sub-objectives a particular task impacted and the fact that many of the organizational type tasks had a wider impact on more of the organizational sub-objectives; the impact of naturally occurring higher global weights as a result of there being less technical objectives was diminished substantially.

6.4 Directions for Future Research

The decision model created in this research resulted from one organizational study and used only three individuals to represent the values of this single organization. And although a comprehensive list of security objectives and subsequent list of 69 value-driven tasks were identified, further research is needed to determine if a more exhaustive list of security objectives and tasks would result from probing the values of additional individuals from this organization.

Secondly, similar studies should be conducted in other organizations to determine additional security objectives and subsequent value-driven tasks. The results of these studies could then be analyzed to determine if similarities exist between organizations in both same and differing sectors of the business world in terms of specific objectives, weights, evaluation measures, value functions, tasks and task rankings. Only through this additional research could the IS research community expect to be able to develop better theories surrounding IS security that consider both technical and organizational issues.

Third, the results of this research lend promise to the notion of being able to create automated auditing tools in the future that assess current states of IS security and provide aid in the decision making process for maximizing IS security from a combined technical and organizational perspective. Of course, the strength of any automated tool would be a function of the amount of research that is used as input. If future research suggests that many similarities exist in terms of security objectives and value-driven tasks across industries, then the amount of work that is needed from a specific organization with any auditing tool would be minimized. However, if future research suggests that security objectives and tasks differ substantially across various organizations and business sectors, then future auditing tools would have to be created in a more generic manner and would require more direct input from any particular organization that may desire the use of such auditing tools.

Fourth, the results of this research provided 69 value-driven tasks along with relationships identifying the various objectives that these tasks impact. Thus empirical work to validate and determine the strength of these relationships should be investigated.

And finally, because many IS-related problems concern the interaction of both technical and organizational issues, the 10-step methodology employed in this research should be investigated and even used for quantifying other IS-related problems that may have been solved in a more subjective manner in the past. For example, the 10-step methodology used in this research could be used to choose among differing ERP solutions for an organization. That is, once an objectives hierarchy is created that relates the values of an organization to its ERP requirements, then the subsequent evaluation measures, value functions, and weights could then be derived to select amongst differing ERP alternatives.

References

Amoroso, E. (1994). "Fundamentals of Computer Security Technology." AT&T Bell Laboratories.

Armstrong, H. (1999). "A soft approach to management of information security." School of Public Health. Curtin University. Perth, Australia, Unpublished PhD Thesis 343.

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

Bagchi, K. and G. Udo (2003). "An analysis of the growth of computer and Internet security breaches." *Communications of AIS* 12, 684–700.

Bargh, J. A. and Gollwitzer, P. (1994). Environmental Control of Goal-Directed Action: Automatic and Strategic Contingencies between Situations and Behavior, in Integrative Views of Motivation, Cognition, and Emotion, ed. William D. Spaulding, Lincoln: University of Nebraska Press, 71-124.

Bargh, J. A. and Chartrand, T. L. (1999). The Unbearable Automaticity of Being, *American Psychologist*, 54 (July), 462-479.

Baskerville, R. (1991). "Risk analysis: an interpretive feasibility tool in justifying information systems security." *European Journal of Information Systems* 1(2): 121-130.

Baskerville, R. (1992). "The developmental duality of information systems security." *Journal of Management Systems* 4(1), 1–12.

Baskerville, R. (1993). "Information systems security design methods: implications for information systems development." *ACM Computing Surveys* 25(4): 375-414.

Bell, D. and LaPadula, L. (1973). "Secure computer systems: Mathematical foundations." Technical Report ESD-TR-73-278, The MITRE Corporation, Bedford, MA.

Bishop, M. (2002). Computer Security: Art and Science. Addison-Wesley-Longman, Boston, MA.

Boockholdt, J. L. (1987). "Security and integrity controls for microcomputers: A summary analysis." *Information and Management,* 13(1): 33-41.

Borcherding, K., Eppel, T., and Von Winterfeldt, D., (1991). Comparison of Weighting Judgments in Multiattribute Utility. *Management Science*, 37, 12, 1603 – 1619.

Chambal, S., Shoviak, M., and Thal, A. E. (2003). "Decision Analysis Methodology to Evaluate Integrated Solid Waste Management Tasks." *Environmental Modeling and Assessment,* 8: 25-34.

Clemen, R. T. (1996). *Making Hard Decisions: An Introduction to Decision Analysis* (2nd Edition). Belmont, CA: Duxbury Press.

Clements, D. P. (1977). Fuzzy ratings for computer security evaluation. University of California, Berkeley. Unpublished PhD Thesis.

Courtney, R. (1997). "Security risk analysis in electronic data processing." Proceedings of the AFIPS, pp. 97 – 104.

Curtin, L. (2000). "On being a person of integrity...or ethics and other liabilities." *Journal of Continuing Education in Nursing*, 31(2): 55-8.

Dhillon, G. (2008). "Organizational competence in harnessing IT: a case study". *Information & Management.* Vol. 45.

Dhillon, G. (2001). "Violation of safeguards by trusted personnel and understanding related information security concerns*."* *Computers & Security*, Vol 20, No 2.

Dhillon, G., and Backhouse, J. (2000). "Information system security management in the new millennium." *Communications of the ACM*, 43, 7:125-128.

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards socio-organizational perspectives." *Information Systems Journal* 11(2): 127-153.

Dhillon, G and Moore, S. (2001) "Computer Crime: theorizing about the enemy within". *Computers & Security*, Vol 20, No 8.

Dhillon, G. and Torkzadeh, R. (2006). "Value focused assessment of information system security in organizations." *Information Systems Journal,* 16, 293–314.

Dunn, R. (1990). "Data integrity and executive information systems." *Computer Control Quarterly,* 8: 23-25.

Emery, F. (1981). Open systems thinking. Volumes I & II. Penguin.

Frisinger, A. (2001). "Improving the protection of assets in open distributed systems by use of X-ifying risk analysis." *Proceedings of the IFIP TC11 Sixteenth International Conference on Information Security*: Paris, France.

Gabaix, X. and Laibson, D. (2000). A Boundedly Rational Decision Algorithm," *American Economic Review*, 90 (May), 433-438.

Gawande, A. (2002). *Complications: A surgeon's notes on an imperfect science.* New York: Metropolitan Books.

Goldstein, D. G., and Gigerenzer, G. (2002). Models of ecological rationality: The recognition heuristic. *Psychological Review, 109,* 75-90.

Guarro, S. (1987). "Principles and procedures of the LRAM approach to information systems risk analysis and management." *Computer and Security* 6(6), 493–504.

Halliday, S., Badenhorst, K. and Von Solms R (1996). "A business approach to effective information technology risk analysis and management." *Information Management and Computer Security,* 4(1), 19–31.

Herrmann, G. and Pernul, G. (1998). "Viewing business process security from different perspectives," *11th International Bled Electronic Commerce Conference*, Slovenia.

Hitchings, J. (1996). A practical solution to the complex human issues of information security design. *Information systems security: facing the information society of the 21st century*. S. K. Katsikas and D. Gritzalis, (Ed.). London, Chapman and Hall: 3-12.

Hitchings, J. (1995). "Deficiencies of the traditional approach to information security and the requirements for a new methodology." *Computers & Security*, Vol. 14, pp. 377-83.

Hutt, A., Hoyt, D. and Bosworth, S. (1998). Computer Security Handbook, 2nd Edn. Macmillan, New York.

IBM. (1972). Secure Automated Facilities Environment Study 3, Part 2. IBM. Armonk, NY.

James, H. L. (1996). "Managing information systems security: a soft approach." *iscnz*, p. 10, *Information Systems Conference of New Zealand* (ISCNZ '96).

Kahneman, D. (2003). "A perspective on judgment and choice: Mapping bounded rationality." *American Psychologist, 58,* 697-720.

Kahneman, D., and Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin, and D. Kahneman (Eds.), *Heuristics and biases* (pp. 49–81). New York: Cambridge University Press.

Kahneman, D., and Tversky, A. (1979). Prospect theory: An analysis of decisions under risk. *Econometrica, 47,* 263–291.

Karyda, M., Kokolakis, S. and Kiountouzis, E. (2003). Content, context, process analysis of IS security policy formulation. *Security and privacy in the age of uncertainty*. D. Gritzalis, S. D. C. d. Vimercati, P. Samarati and S. Katsikas, (Ed.). Boston, Kluwer Academic Publishers: 145-156.

Keeney, R. L. (1992). *Value-focused thinking*. Cambridge, Massachusetts, Harvard University Press.

Keeney, R. L. and Raiffa, H. (1993). *Decsions with Multiple Objectives*. Cambridge, Massachusetts, Cambridge University Press.

Keeney, R. L. (1994). "Creativity in Decision Making with Value-Focused Thinking." *Sloan Management Review*, 35: 33-41.

Kirkwood, Craig W. (1997). *Strategic Decision Making, Multiobjective Decision Analysis with Spreadsheets*. Belmont: Wadsworth Publishing Company.

Klein, G. (1998). *Sources of power: How people make decisions.* Cambridge, MA: MIT Press.

Klein, G. (2003). *Intuition at work: Why developing your gut instincts will make you better at what you do.* New York: Doubleday.

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Morrow, D. W. (2006). The Top Information Security Issues Facing Organizations: What Can Government do to Help? *Information Systems Security*, Sep/Oct 15:4 51-58.

Kraus, L. (1972). SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems. Amacom, New York.

Lee, A. S. (2003). "Re-introducing the systems approach to information systems." Keynote address at *ISOneWorld*, Las Vegas, NV.

Lee, A.S. (2004). "Thinking about Social Theory and Philosophy for Information Systems." In *Social Theory and Philosophy for Information Systems*, edited by Mingers, J., Willcocks, L., John Wiley and Sons.

Louis, M. R. and Sutton, R. L. (1991). Switching Cognitive Gears: From Habits of Mind to Active Thinking, *Human Relations*, 44 (January), 55-76.

Maletic, J. I. and Marcus, A. (2000). "Data Cleansing: Beyond Integrity Analysis ." In *Proceedings of The Conference on Information Quality*.

McGrath, R., Gunther, I., MacMillan, C. and Venkataraman, S. (1995). "Defining and Developing Competence: A Strategic Process Paradigm." *Strategic Management Journal,* 16.4 (1995): 251-75.

Merrick, J. R. and Garcia, M. W. (2004). "Using Value-Focused Thinking to Improve Watersheds." *Journal of the American Planning Association* 70(3): 313 – 337.

Moulton, R. and Moulton M. (1996). "Electronic communications risk management: a checklist for business managers." *Computer and Security,* 15(5), 377–386.

Phythian, G. J., and King, M. (1992). "Developing an Expert Support System for Tender Enquiry Evaluation: A Case Study." *European Journal of Operations Researc*h, Vol. 56, pp. 15-29.

Rainer, R. K., Marshall, T. E., Knapp, K. J., and Mongomery, G. H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? *Information Systems Security*, Mar/Apr 16:2 100-108.

Ronis, D. L., Yates, J., and Kirscht, J. P. (1989). Attitudes, Decisions, and Habits as Determinants of Repeated Behavior, in *Attitude Structure and Function*, ed. Anthony R. Pratkanis et al., Hillsdale, NJ: Erlbaum, 213-239.

Saaty, T. (1980). *The Analytical Hierarchy Process.* NY, NY, McGraw-Hill, International.

Sandhu, R.S. and Samarati (1994). Access Control: Principles and Practice, Communications Magazine, IEEE, 32:9 (September) : 40-48.

Schneider, W. and Shiffrin, R. (1977). Controlled and Automatic Human Information Processing. I. Detection, Search and Attention, *Psychological Review*, 84 (January), 1-66.

Segev, A., Porra, J. and Roldan, M. (1998). "Internet security and the case of Bank of America." *Communications of the ACM* 41(10): 81-87.

Shiffrin, R. M. and Schneider, W. (1977). Controlled and Automatic Human Information Processing. II. Perceptual Learning, Automatic Attending and a General Theory," *Psychological Review*, 84 (March), 127-190.

Simon, H. A., and Chase, W. G. (1973). Skill in chess. *American Scientist, 61,* 394–403.

Siponen, M. T. (2001). "An analysis of the recent IS security development approaches: descriptive and prescriptive implications." *Information security management: global challenges in the new millennium*. G. Dhillon, (Ed.). Hershey, Idea Group Publishing: 101-124

Siponen, M. T. (2005). "An analysis of the traditional IS security approaches: implications for research and practice." *European Journal of Information Sytems,* 14(10): 303-315.

Sloman, S. A. (2002). Two systems of reasoning. In T. Gilovich, D. Griffin, and D. Kahneman (Eds.), *Heuristics and biases* (pp. 379–396). New York: Cambridge University Press.

Stanovich, K. E., and West, R. F. (1999). Discrepancies between normative and descriptive models of decision making and the understanding/acceptance principle. *Cognitive Psychology, 38,* 349–385.

Stanovich, K. E., and West, R. F. (2002). Individual differences in reasoning: Implications for the rationality debate. In T. Gilovich, D. Griffin, and D. Kahneman (Eds.), *Heuristics and biases* (pp. 421–440). New York: Cambridge University Press.

Straub, D. W. and R. J. Welke (1998). "Coping with systems risks: security planning models for management decision making." *MIS Quarterly* 22(4): 441-469.

Strens, R. and Dobson, J. (1993). "How responsibility modeling leads to security requirements." *Proceeding of the 16th National Computer Security Conference*, Baltimore, MD, pp. 398 – 408.

Tversky, A., and Kahneman, D. (1986). "Rational choice and the framing of decisions." *Journal of Business, 59,* S251–S278.

Trompeter, C. M. and J. H. P. Eloff (2001). "A framework for implementation of socio-ethical controls in information security." *Computers and Security* 20(5): 384-391.

U.S. Code, (2006). 44 U.S.C. § 3542 (b)(1). http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-.html

Willcocks, L. and H. Margetts (1994). "Risk assessment and information systems." *European Journal of Information Systems* 3(2): 127-139.

Wilson, T. D., and Schooler, J. W. (1991). Thinking too much: Introspection can reduce the quality of preferences and decisions. *Journal of Personality and Social Psychology, 60,* 181–192.

Wing, J. M. (1998). A Symbiotic Relationship between Formal Methods and Security. Proceedings from Workshops on Computer Security, Fault Tolerance, and Software Assurance: From Needs to Solution. CMU-CS-98-188, December.

Appendix A: Generic Evaluation Measures

Table A.1: Generic Evaluation Measures for Enhance Management Development Practices

1. Enhance management development practices		
Sub-Objective	**Evaluation Measure**	
1.1 Develop a management team that leads by example	**M**	You or your management team attempt to develop an environment that leads by example.
	O	You feel that your management team attempts to develop an environment that leads by example.
1.2 Ensure individual comfort level of computers/software	**M**	You or your management team has made an effort to make your subordinates feel comfortable with using the basic features of their computers.
	M	You or someone you know has made an effort to make your subordinates feel comfortable with using the basic features of the software that they are required to use.
	MO	You feel comfortable using the basic features of your computer.
1.3 Increase confidence in using computers	**M**	You or your management team has made an effort to make your subordinates feel confident about using their computers.
	MO	You feel confident using your computer.
1.4 Create legitimate opportunities for financial gain	**MO**	You understand the importance of computer technology and how it is related to the financial well-being of your organization.
1.5 Provide employees with adequate IT training	**M**	You or your management team have attempted to provide your subordinates with adequate IT training.
	O	You feel as if you have received adequate IT training.
1.6 Develop capability level of IT staff	**M**	You or your management team attempt to develop the capability level of the IT staff.
	MO	You feel as if the IT staff of your IT department is capable of handling the technology needs of your organization.

Table A.2: Generic Evaluation Measures for Provide Adequate Human Resource Management Practices

2. Provide adequate human resource management practices		
Sub-Objective	**Evaluation Measure**	
2.1 Provide necessary job resources	**M**	You or your management team attempt to provide necessary job resources to your employees.
	O	You feel as if the necessary job resources have been provided to you to be efficient in completing your job responsibilities.
2.2 Create an environment that promotes contribution	**M**	You or your management team attempt to create an environment where your subordinates desire to contribute.
	O	You feel as if you work in an environment that promotes contribution.
2.3 Encourage high levels of group morale	**M**	You or your management team attempt to create an environment that encourages high levels of morale.
	O	You feel as if you work in an environment that promotes high levels of morale.
2.4 Enhance individual/group pride in the organization	**M**	You or your management team attempt to create an environment that enhances individual or group pride in the organization.
	O	You feel you work in an environment that promotes pride in the organization.
2.5 Create an environment of employee motivation	**M**	You or your management team attempt to create an environment that encourages motivation amongst your employees.
	O	You feel you work in an environment that promotes pride in the organization.
2.6 Create an organizational code of ethics	**M**	You or your management team have created and made known an organizational code of ethics.
	O	You have been made aware of and understand your organizational code of ethics.

Table A.3: Generic Evaluation Measures for Develop and Sustain an Ethical Environment

3. Develop and sustain an ethical environment		
Sub-Objective	**Evaluation Measure**	
3.1 Develop an understood value system in the organization/whistle blowing	**M**	You or your management team attempt to provide an understanding of the values of your organization to your employees.
	O	You feel that you understand the values of your employees.
3.2 Develop co-worker and organizational ethical relationships	**M**	You or your management team attempt to develop co-worker and organizational ethics.
	O	You feel as if you have been made to understand the importance of maintaining good co-worker relationships.
3.3 Instill value-based work ethics	**M**	You or your management team attempt to instill value-based work ethics to your employees.
	O	You feel as if you have been made to understand value-based work ethics in your organization.
3.4 Instill professional work ethics	**M**	You or your management team attempt to instill professional based work ethics to your employees.
	O	You feel as if you have been made to understand professional based work ethics in your organization.
3.5 Create an environment that promotes organizational loyalty	**M**	You or your management team attempt to create an environment that promotes organizational loyalty.
	O	You feel you work in an environment that promotes organizational loyalty.
3.6 Stress individuals treating others as they would like to be treated	**M**	You or your management team attempt to provide an understanding of the importance of treating others as they would like to be treated.
	O	You feel that you have been made aware by management of the importance of treating others as they would like to be treated.

Table A.4: Generic Evaluation Measures for Maximize Access Control

4. Maximize access control		
Sub-Objective	**Evaluation Measure**	
4.1 Create user passwords	**MO**	You feel as if the sensitive data in your organization is adequately protected by passwords.
4.2 Provide several levels of user access	**M**	You feel that your organization provides the necessary levels of user access to pertinent data for your employees.
	O	You feel that your organization provides you with the necessary access to pertinent data to complete your job responsibilities.
4.3 Ensure physical security	**MO**	You feel that the technology within your organization is physically secure.
4.4 Minimize unauthorized access to information	**M**	You feel that your employees do not have the ability to access information that is not pertinent to their job.
	O	You are not able to access sensitive data that is not pertinent to your job.

Table A.5: Generic Evaluation Measures for Promote Individual Work Ethic

5. Promote individual work ethic		
Sub-Objective	**Evaluation Measure**	
5.1 Maximize employee integrity in the company	**M**	You or your management team attempt to create an environment that maximizes employee integrity in the organization.
	O	You feel as if you work in an environment that emphasizes employee integrity in the organization.
5.2 Minimize urgency of personal gain	**M**	You or your management team attempt to create an environment that minimizes the urgency of personal gain.
	O	You feel as if you work in an environment that minimizes the urgency of personal gain.
5.3 Create a desire to not jeopardize the position of the company	**M**	You or your management team attempt to create an environment that creates a desire to not jeopardize the position of the company.
	O	You feel as if you work in an environment that emphasizes a desire to not jeopardize the position of the company.
5.4 Create an environment that promotes company profitability rather than personal gain	**M**	You or your management team attempt to create an environment that promotes company profitability rather than personal gain.
	O	You feel as if you work in an environment that promotes company profitability rather than personal gain.
5.5 Minimize temptation to use information for personal benefit	**M**	You or your management team attempt to create an environment that minimizes the temptation of your employees to use information for personal benefit.
	O	You feel as if you work in an environment that minimizes the temptation for you to use information for personal benefit beyond what is required for your job.

Table A.6: Generic Evaluation Measures for Maximize Data Integrity

6. Maximize data integrity		
Sub-Objective	**Evaluation Measure**	
6.1 Minimize unauthorized changes	**MO**	You feel as if the sensitive data in your organization is adequately protected against unauthorized changes.
6.2 Ensure data integrity	**MO**	You feel as if the integrity of pertinent data within your organization is maintained in a satisfactory manner.

Table A.7: Generic Evaluation Measures for Enhance Integrity of Business Processes

7. Enhance integrity of business processes		
Sub-Objective	**Evaluation Measure**	
7.1 Understand the expected use of all available information	**M**	You or your management team attempt to provide an environment where your employees understand the expected use of available information.
	O	You feel as if you understand the expected use of available information.
7.2 Develop understanding of procedures and codes of conduct	**M**	You or your management team attempt to help your employees understand procedures and codes of conduct.
	O	You feel as if you understand procedures and codes of conduct within your organization.
7.3 Ensure that appropriate organizational controls (formal and informal) are in place	**M**	You or your management team have developed appropriate organizational controls and made them understandable to your employees.
	O	You feel as if you have an accurate understanding of the controls set forth by your organization.

Table A.8: Generic Evaluation Measures for Maximizing Privacy

8. Maximizing privacy		
Sub-Objective	**Evaluation Measure**	
8.1 Emphasize importance of personal privacy	**M**	You or your management team attempt to emphasize the importance of personal privacy to your employees in terms of sensitive data.
	O	You feel as if your organization has emphasized the importance of personal privacy of sensitive data.
8.2 Emphasize importance of rules against disclosure	**M**	You or your management team attempt to emphasize the importance of rules against unethical or unlawful disclosure of private data.
	O	You feel as if your organization has emphasized the importance of rules against unethical or unlawful disclosure of private data.

Table A.9: Generic Evaluation Measures for Maximize Organizational Integrity

9 Maximize organizational integrity		
Sub-Objective	**Evaluation Measure**	
9.1 Create an environment of managerial support and solidarity	**M**	You or your management team attempt to create an environment of managerial support and solidarity.
	O	You feel as if you work in an environment of managerial support and solidarity.
9.2 Create environment of positive management interaction	**M**	You or your management team attempt to create an environment of positive management interaction.
	O	You feel as if you work in an environment of positive management interaction.
9.3 Create an environment that promotes respect	**M**	You or your management team attempt to create an environment that promotes respect.
	O	You feel as if you work in an environment that promotes respect amongst you and your co-workers.
9.4 Create an environment that promotes individual reliability	**M**	You or your management team attempt to create an environment that promotes individual reliability.
	O	You feel as if you work in an environment that promotes individual reliability.
9.5 Create environment of positive peer interaction	**M**	You or your management team attempt to create an environment of positive peer interaction.
	O	You feel as if you work in an environment of positive peer interaction.

Appendix B: Documentation of Meetings with Organization

Meeting 1 - Introduction

Location: MSI Corp
Attendees: Jeffrey May, Gurpreet Dhillon, Carolyn Strand Norman, Auditor 1, Auditor 2, and Auditor 3 (**Team** = Auditor 1 + Auditor 2 + Auditor 3)

Purpose: To introduce the Team to Gurpreet and Jeff via Carolyn and to introduce the research approach and types of results we hope to achieve. We also wanted to secure a commitment from the Team to do this research for IRB purposes.

The following 1-page handout was created and discussed:

Developing a Decision Model for IS Security

– A Virginia Commonwealth research project –

Due to the overwhelming and often times misunderstood issues that require attention, information system (IS) security continues to present a major challenge to organizations. In a recent survey, 75% of all organizations reported some type of security attack. Obviously, security attacks can not only be costly, but can also shut down an organization's information system. As a result, this research will develop and validate a theoretically and methodologically sound decision model that will provide a consistent and scalable means for generating informed alternatives to decision makers for the purpose of maximizing IS security in an organization.

What Is This Project About?

In a recent research effort, Dhillon and Torkzadeh (2006) compiled a list of fundamental objectives that were found by directly probing the implicit values of decision makers responsible for maintaining IS security across various industry segments. These objectives provide the IS research community with am exhaustive list of both technical and organizational issues for addressing IS security. However, without providing direction for creating, evaluating and selecting alternatives, the results of their exhaustive research efforts are limited in their practical capacity to provide decision makers with the ability to make informed decisions. Therefore the objective of this research is to develop a methodologically sound decision model for creating, evaluating and selecting the best alternatives in the context of maximizing IS security within an organization.

What Benefits Will Be Derived From This Research?

This research project will provide the following benefits to the organization studied:

- An exhaustive list of security objectives that require attention along with their associated degree of importance (weights) for the specific organization to be studied.
- An exhaustive list of evaluation measures for the various security objectives.
- An exhaustive and ranked list of alternatives (i.e., ideas, concepts, tasks and solutions) that should be employed by the organization to maximize IS security.

Deliverables: A detailed report of findings along with final recommendations will be presented to the organization at the completion of this research. The format of the report will depend on the insights gained during the analysis and the questions posed by the decision model.

Who Should You Contact?

If you are interested in obtaining more detail about this research project, please contact:

- Dr Gurpreet Dhillon (gdhillon@vcu.edu)
- Jeffrey May (jmay@isy.vcu.edu)
- Dr. Carolyn Strand Norman (castrand@vcu.edu)

Commitment from the Team:

This email is to confirm that this organization has agreed to work with Jeffrey May and Gurpreet Dhillon on the research project titled, "Developing a Multi-objective Decision Model for Maximizing IS Security within an Organization." This research will be used for Jeffrey May's dissertation and may produce future publications. The organization's name will not be used in any publications unless there is a mutual agreement between the organization and Jeffrey May.

Auditor 1
SVP & General Auditor
Audit & Advisory Resources

Time Commitment Email:

Auditor 1, many thanks for being such a big help in carrying forward our research. I am sure that it will be mutually beneficial. Your 20-30 hr estimate is spot on. We will try to be as efficient as possible.

Jeffrey May

Meeting 2 - Value Hierarchy, Evaluation Measures, and Value Functions

Location: MSI Corp
Attendees: Jeffrey May, Gurpreet Dhillon, Auditor 1, Auditor 2, and Auditor 3 (Team).

Purpose: To determine appropriate evaluation measures and value functions and to familiarize the team with the fundamental objectives. Via this process, the fundamental objectives will be verified or amended to the exact values of the organization.

Thoughts: The meeting went rather smoothly. The Team worked very hard to come up with understandable evaluation measures which subsequently forced them to think of the importance of each sub-objective as it relates to Information System Security. Obviously, this will pay dividends when attempting to weight each sub-objective relative to its peers. A few sub-objectives were changed in terms of wording and many times as each sub-objective was introduced, the Team met it with initial skepticism but usually through interaction, found a relationship. We were only able to get through 2 main objectives this day but in hindsight this initial process of familiarization probably will take longer than originally expected.

First Objective Discussed: Promote individual work ethic

Table B.1: Verified or Amended Objectives and Evaluation Measures for Promote Individual Work Ethic

Maximize employee integrity in the company	**M**	You or your management team creates an environment that maximizes employee integrity in the organization.
	O	You feel as if you work in an environment that emphasizes employee integrity in the organization.
Create a desire to not jeopardize the reputation of the company	**M**	You or your management team creates an environment that promotes a desire to not jeopardize the reputation of the company.
	O	You feel as if you work in an environment that emphasizes a desire to not jeopardize the reputation of the company.
Create an environment that promotes the organization's best interests rather than personal gain.	**M**	You or your management team creates an environment that promotes the organization's best interests rather than personal gain.
	O	You feel as if you work in an environment that promotes the organization's best interests rather than personal gain.
Minimize temptation to use information for personal benefit	**M**	You or your management team creates an environment that minimizes the temptation of your employees to use information for personal benefit.
	O	You feel as if you work in an environment that minimizes the temptation for you to use information for personal benefit.

Notes for above:

- The Team felt that Minimize opportunity of personal gain is an Access Control Issue and was thus removed.
- The Team examined these sub-objectives from the context of creating evaluation measures and by considering what they called TASKS to accomplish each sub-objective
    - TASKS → Alternatives; Practice → Theory
- Via this type of examination, the wording of the above sub-objectives changed
- The Team seemed to understand that this process was needed for creating a decision model but started to get a touch restless as this process was somewhat taxing to them.
- I tried to keep the Team centered on the individual sub-objective rather than focusing on the big and complicated picture

Second Objective Discussed: Develop and sustain an ethical environment

Table B.2: Verified or Amended Objectives and Evaluation Measures for Develop and Sustain an Ethical Environment

Create an environment that makes it ok to report unethical behavior (whistle blowing)	**M**	You or your management team creates an environment that makes it ok to report unethical behavior (whistle blowing)
	O	You feel that you have been made aware of the importance of reporting unethical behavior
Develop an understood value system in the organization	**M**	You or your management team has created a value system that you make known to your employees.
	O	You feel that you understand the values of your organization.
~~Discourage unethical relationships~~	~~**M**~~	~~You or your management team creates an environment that discourages unethical relationships on the job (business, personal)~~
	~~**O**~~	~~You feel as if you have been discouraged to interact in unethical relationships (business, personal) on the job~~
~~Instill value-based work ethics~~	~~**M**~~	~~You or your management team instills value-based work ethics to your employees (i.e. company values).~~
	~~**O**~~	~~You feel as if you have been made to understand value-based work ethics in your organization (i.e. company values).~~
~~Instill professional-based work ethics~~	~~**M**~~	~~You or your management team attempt to instill professional-based work ethics to your employees.~~
	~~**O**~~	~~You feel as if you have been made to understand professional-based work ethics in your organization.~~
Create an environment that promotes organizational loyalty	**M**	You or your management team creates an environment that promotes organizational loyalty.
	O	You feel you work in an environment that promotes organizational loyalty.
~~Stress individuals treating others as they would like to be treated~~	~~**M**~~	~~You or your management team attempt to provide an understanding of the importance of treating others as they would like to be treated.~~
	~~**O**~~	~~You feel that you have been made aware by management of the importance of treating others as they would like to be treated.~~
Ensure adequate management oversight of developing and sustaining an ethical environment	**MO**	You feel that your organization ensures adequate management oversight of organizational integrity issues.

Notes for above:

- The Team originally felt that Develop an understood value system in the organization/ whistle blowing needed to be broken down into two sub-objectives
- The Team indicated that they felt that these sub-objectives were environment based where the previous sub-objectives were more individual based
- Many times, the team had trouble relating these objectives to IS Security but on each occasion, we were able to see a relationship, although they thought it was minor
    - It could be that this objective has a small weight when compared to the other 9…. **Keep this mind when we weight!**
- All ~~objectives~~ were later considered to be tasks.

Third Objective Discussed: Enhance management development practices

Notes for above:

- We were not able to complete this objective.
- The Team wants to change the main objective from Enhance management development practices to Maximize IT competence
- The Team has originally indicated the sub-objective, Develop a management team that leads by example may need to be placed in the ethics related objectives as it seems to not be related to the rest of these sub-objectives or to IT competence

Final Notes:

- The Team and I were definitely tired at the end of the session and I felt that they were a bit skeptical of this whole process. Maybe I was skeptical?? After having some time to think, I really believe that we are making ground and that some excellent insight was provided by the Team. I really believe that we are on our way!
- I followed up the meeting with the below email and am waiting for a time from Auditor 1 for our next meeting. Unfortunately, I was not able to get a next meeting scheduled while I was there. This was probably because I was tired.

Follow up Email:

Hi Auditor 1,

I just wanted you to know that our first meeting accomplished exactly what I was hoping for. That is, we really thought about the importance of each sub-objective and although some were met with skepticism, this is exactly what we want. These original meetings will certainly provide us the insight to appropriately weight each objective as they relate to IS Security in your organization. I really appreciate the hard thinking of the MSI Corp team. Of course, we did not progress as fast as I was hoping, but in hindsight, I am thinking that the better we do at this stage, the easier and more correct the later stages will be. I look forward to our next meeting.

Sincerely ,Jeff

Meeting 3 - Value Hierarchy, Evaluation Measures, and Value Functions
Location: MSI Corp
Attendees: Jeffrey May, Auditor 1, Auditor 2, and Auditor 3 (Team).

Purpose: To continue to determine appropriate evaluation measures and value functions and to familiarize the team with the fundamental objectives.

Thoughts: We learned from our last meeting that we should verify various sub-objectives by considering both evaluation measures and tasks to attain or implement these sub-objectives. By considering tasks, we were able to make sense of many sub-objectives. We also found that some of the sub-objectives were in fact tasks, thus they were either amended or removed.

Third Objective Discussed: Enhance management development practices

Changed to: Maximize IT Competence

Table B.3: Verified or Amended Objectives and Evaluation Measures for Maximize IT Competence

Develop a management team that leads by example	**M**	You or your management team leads by example for the purpose of maximizing IT competence.
	O	You feel that your management team leads by example for the purpose of maximizing IT competence.
Increase confidence/comfort level in using computers	**M**	You or your management team provides an environment that increases individual confidence/comfort level with computer technology.
	MO	You feel as if your management team provides an environment that increases individual confidence/comfort level with computer technology.
Maximize understanding the importance of computer technology and how it is related to the financial well-being of your organization	**MO**	You understand the importance of computer technology and how it is related to the financial well-being of your organization
Ensure employees have adequate IT training	**M**	You or your management team provides IT training opportunities.
	O	You feel as if you have adequate opportunities for IT training.
Ensure IT capability level of staff	**M**	You or your management team ensures a proper level of IT capability amongst your staff.
	O	You feel as if you and your peers have an adequate level of IT capability.

Notes for above:

- The Team had originally indicated the sub-objective, Develop a management team that leads by example may need to be placed in the ethics related objectives as it seems to not be related to the rest of these sub-objectives or to IT competence
    - During this meeting they decided to keep it here but will probably give it a low weight.
- Confidence and comfort were combined (redundant) as the Team could not distinguish between the two when considering tasks.
- The sub-objective, Create legitimate opportunities for financial gain was considered a weak objective in this mix and may be given a low weight.

Fourth Objective Discussed: Maximizing Privacy

Changed to: Maximize Privacy

Table B.4: Verified or Amended Objectives and Evaluation Measures for Maximize Privacy

Emphasize importance of data privacy	**M**	You or your management team emphasizes the importance of data privacy to your employees.
	O	You feel as if your organization has emphasized the importance of data privacy.
Ensure employee awareness against disclosure of sensitive data	**M**	You or your management team emphasizes the importance of rules against unethical or unlawful disclosure of sensitive data.
	O	You feel as if your organization has emphasized the importance of rules against unethical or unlawful disclosure of sensitive data.
Ensure employees understand the repercussions of disclosing sensitive data	**M**	You or your management team emphasize the importance of understanding the repercussions of disclosing sensitive data
	O	You feel as if your organization has emphasized the importance of understanding the repercussions of disclosing sensitive data
Ensure that sensitive data is adequately secured	**M**	You or your management team ensures that sensitive data is adequately secured.
	O	You feel as if your organization ensures that sensitive data is adequately secured.
Ensure adequate management oversight of privacy issues	**MO**	You feel that your organization ensures adequate management oversight of privacy issues.

Notes for above:

- May be many tasks/alternatives for Ensure that sensitive data is adequately secured
- The Team did not feel that the the original sub-objectives adequately covered this fundamental objective (not collectively exhaustive). Thus, new sub-objectives were added.

Fifth Objective Discussed: Provide adequate human resource management practices

Changed to: Promote Employee Development and Management Practices

Table B.5: Verified or Amended Objectives and Evaluation Measures for Promote Employee Development and Management Practices

~~Provide necessary resources/tools to perform job functions~~	~~**M**~~	~~You or your management team provides to your employees the necessary resources/tools to perform job functions.~~
	~~**O**~~	~~You feel as if the necessary resources/tools to perform job functions have been provided to you to be efficient in completing your job responsibilities.~~
Create an environment that promotes contribution	**M**	You or your management team creates an environment where your subordinates desire to contribute
	O	You feel as if you work in an environment that promotes contribution.
Instill high levels of morale	**M**	You or your management team create an environment that instills high levels of morale
	O	You feel as if you work in an environment that instills high levels of morale.
Increase/maintain pride in the organization	**M**	You or your management team creates an environment that Increases/maintains pride in the organization.
	O	You feel you work in an environment that increases/maintains pride in the organization.
Develop and maintain a motivated workforce	**M**	You or your management team creates an environment that develops and maintains a motivated workforce.
	O	You feel you work in an environment that develops and maintains a motivated workforce.
~~Create/maintain/make known an organizational code of ethics~~	~~**M**~~	~~You or your management team have created/maintained/made known an organizational code of ethics.~~
	~~**O**~~	~~You have been made aware of and understand your organizational code of ethics.~~

Notes for above:

- Possibly a low weight for create/maintain/make known an organizational code of ethics
- Provide necessary resources/tools to perform job functions is a task and was removed
- Create/maintain/make known an organizational code of ethics is a task and was removed.

Meeting 4 - Value Hierarchy, Evaluation Measures, and Value Functions

Location: Organization
Attendees: Jeffrey May, Auditor 1, Auditor 2, and Auditor 3 (Team).

Purpose: To finish determining appropriate evaluation measures and value functions and to familiarize the team with the fundamental objectives so that weights and tasks can be determined.

Thoughts: Today the team was rather productive and worked extremely hard to finish amending the fundamental objective hierarchy and creating evaluation measures. In hindsight the original fundamental objectives and sub-objectives ended up being a template that spurred creative thinking and rewording of objectives to fit the organization's values. For each sub-objective, tasks or alternatives were considered to make sense of the sub-objective, if no tasks could be thought of, the sub-objective was changed to appropriately match the fundamental objective and to spur value-driven tasks. The team was more positive today than any other day previously and felt as if this research may benefit them.

Additional Note: Make sure that the respondents recognize that we are in no way trying to solve the IS security puzzle; we are only trying to find tasks or alternatives that may not have been recognized previously without the value hierarchy. Any new tasks created or thought of via this process will certainly help in maximizing IS security.

Sixth Objective Discussed: Maximize Access Control

Table B.6: Verified or Amended Objectives and Evaluation Measures for Maximize Access Control

Maintain personal accountability for system use	**MO**	You feel as if personal accountability for access control is maintained at adequate levels.
Ensure appropriate levels of user access	**M**	You feel that your organization provides the appropriate levels of user access to pertinent data for your employees.
	O	You feel that your organization provides you with the appropriate levels of user access to pertinent data.
Ensure appropriate physical security	**MO**	You feel that the technology within your organization is physically secure at an appropriate level.
Ensure user access is based on "need to know"	**M**	You feel that your employees do not have the ability to access information that is not pertinent to their job.
	O	You are not able to access sensitive data that is not pertinent to your job.
Ensure adequate management oversight of access control	**MO**	You feel that your organization ensures adequate management oversight of access control

Notes for above:

- Create user passwords was considered a task for accountability
- Minimize unauthorized access to information was considered a task for accountability
- The notion of creating a management oversight sub-objective for each fundamental objective was discussed.

Seventh Objective Discussed: Maximize Data Integrity

Table B.7: Verified or Amended Objectives and Evaluation Measures for Maximize Data Integrity

Minimize inappropriate changes to data	**MO**	You feel as if the sensitive data in your organization is adequately protected against inappropriate changes.
Ensure appropriate data integrity controls for the processing of data	**MO**	You feel as if adequate controls for the purpose of maintaining the integrity of pertinent data within your organization have been established
Ensure adequate management oversight of data integrity issues	**MO**	You feel that your organization ensures adequate management oversight of data integrity issues.

Notes for above:

- Ensure data integrity was considered the same as the fundamental objective.
- Extra sub-objectives were added

Eighth Objective Discussed: Enhance integrity of business processes

Table B.8: Verified or Amended Objectives and Evaluation Measures for Enhance Integrity of Business Processes

Understand the expected use of available information and its relation to individual business processes	**M**	You or your management team ensure that employees understand the expected use of information and its relation to individual business processes
	O	You feel as if you understand the expected use of available information and its relation to individual business processes
Develop procedures for managing changes to business processes	**M**	You or your management team are aware of or take part in developing procedures for managing changes to business processes
	O	You feel as if you understand the procedures required for changing business processes.
Ensure that appropriate organizational controls are in place	**M**	You or your management team have developed appropriate organizational controls of business processes and made them understandable to your employees.
	O	You feel as if you have an accurate understanding of business process controls set forth by your organization.

Ninth Objective Discussed: Maximize organizational integrity

Table B.9: Verified or Amended Objectives and Evaluation Measures for Maximize Organizational Integrity

Create an environment of managerial support and solidarity	**M**	You or your management team creates an environment of managerial support and solidarity.
	O	You feel as if you work in an environment of managerial support and solidarity.
Create an environment that empowers employees	**M**	You or your management team creates an environment that empowers employees.
	O	You feel as if you work in an environment that empowers you to do what it takes to get the job done.
Create an environment that promotes respect	**M**	You or your management team creates an environment that promotes respect.
	O	You feel as if you work in an environment that promotes respect amonst you and your co-workers.
Create an environment that promotes individual reliability	**M**	You or your management team creates an environment that promotes individual reliability.
	O	You feel as if you work in an environment that promotes individual reliability.
Ensure adequate management oversight of organizational integrity issues	**MO**	You feel that your organization ensures adequate management oversight of organizational integrity issues.

Notes for above:

- Integrity was defined as being able to count on someone to do what is expected. This definition provided a contrast against ethics. In other words you can have integrity but still be unethical.
- Create an environment of managerial support and solidarity may have a high weight
- Create environment of positive management interaction was deemed redundant with Create an environment of managerial support and solidarity and was thus removed
- Create an environment that promotes respect may have a low weight
- Create an environment that promotes individual reliability may have a strong weight
- Create environment of positive peer interaction was deemed redundant with Create an environment that promotes respect and was thus removed.

Meeting 5 - Value Functions

Location: MSI Corp
Attendees: Jeffrey May, Auditor 1, Auditor 2, and Auditor 3 (Team).

Purpose: To create value functions for all of the second tier objectives.

Value Functions: The Team and I discussed in more detail the notion of value functions and determined that all of the second tier objectives required creating a constructed scale. We started out focusing on the first second tier objective for "Maximize IT Competence" namely, "Develop a management team that leads by example." Because there were two evaluation measures for both management and operational employees, we considered the idea of creating two separate value functions. However, we finally decided to create one value function that captured the essence of both evaluation measures as shown below. After we created this first value function, we then created the second and quickly realized that all of the value functions would be created in a similar manner. Thus, the Team decided that it would be best for the researcher to create the remaining value functions using what we learned from this meeting. The Team would then verify these value functions when it came time for scoring the various alternatives.

Table B.10: Evaluation Measures and Value Function for Develop a Management Team that Leads by Example

Evaluation Measures		
M	You or your management team attempt to develop an environment that leads by example.	
O	You feel that your management team attempts to develop an environment that leads by example.	
Point	**Definition**	**Value**
Not at All	If this alternative is implemented to the best of its ability it has no impact on developing a management team that leads by example. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this alternative is implemented to the best of its ability it has a very subtle impact on developing a management team that leads by example. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this alternative is implemented to the best of its ability it has somewhat of an impact on developing a management team that leads by example. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this alternative is implemented to the best of its ability it has a strong but not overwhelming impact on developing a management team that leads by example. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this alternative is implemented to the best of its ability it will have an overwhelming impact on developing a management team that leads by example. Impacts will definitely be realized by both management and operational employees.	**1**

Meeting 6 - Weights

Location: MSI Corp
Attendees: Jeffrey May, Auditor 1

Purpose: To determine weights for all of the objectives. This process was done on an individual basis for Auditor 1.

Notes: To determine weights, we first examined the second tier objectives. To determine these weights, each second tier objective for a particular fundamental objective was examined. The respondent was then asked to imagine each of these objectives at its worst possible level. The respondent was then asked to determine which objective he would like to see swing to its best possible level. After going through this process several times for each branch, we established ranks. The lowest ranked objective was then assigned a value of X and the remaining objectives were assigned multiples of X. For example, objective 1.5 below was considered to be 2.5 times more important than objective 1.1. After these values of X are assigned, weights can easily be determined by recognizing that the sum of the weights in an individual branch must be equal to 1. For example, for "Maximize IT competence":

X+X+X+1.5X+2.5X = 1
→ X = 1/7 = 0.143;
→ **OBJ1.1W** = 0.143; **OBJ1.5W** = 2.5 * 0.143 = 0.357

Table B.11: Weighting Raw Data - Auditor 1

First Tier	Second Tier
1. Maximize IT Competence	1.1 Develop a management team that leads by example **X**
	1.2 Ensure confidence/comfort level in using computers **X**
	1.3 Ensure an adequate understanding the importance of computer technology and how it is related to the financial well-being of your organization **X**
	1.4 Ensure employees have adequate IT training **1.5X**
	1.5 Ensure IT capability level of staff **2.5X**
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution **X**
	2.2 Instill high levels of morale **X**
	2.3 Increase/maintain pride in the organization **X**
	2.4 Develop and maintain a motivated workforce **X**
3. Develop and Sustain an Ethical Environment	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing) **X**
	3.2 Develop and/or make known an understood value system in the organization **3X**
	3.3 Create an environment that promotes organizational loyalty **1.5X**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment **2X**
4. Maximize Access Control	4.1 Ensure personal accountability for system use **X**
	4.2 Ensure appropriate levels of user access **1.5X**
	4.3 Ensure appropriate physical security **1.75X**
	4.4 Ensure user access is based on "need to know" **1.5X**
	4.5 Ensure adequate management oversight of access control issues. **X**
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company **2.5X**
	5.2 Create a desire to not jeopardize the reputation of the company **X**
	5.3 Create an environment that promotes the organization's best interests rather than personal gain. **X**
	5.4 Minimize temptation to use information for personal benefit **1.5X**
6. Maximize Data Integrity	6.1 Ensure that inappropriate changes to data are minimized **2X**
	6.2 Ensure appropriate data integrity controls for the processing of data **1.5X**
	6.3 Ensure adequate management oversight of data integrity issues **X**
7. Enhance Integrity of Business Processes	7.1 Ensure an understanding of the expected use of available information and its relation to individual business processes **1.5X**
	7.2 Develop procedures for managing changes to business processes **X**
	7.3 Ensure that appropriate organizational controls are in place **2X**
8. Maximize Privacy	8.1 Emphasize importance of data privacy **1.75X**
	8.2 Ensure employee awareness against disclosure of sensitive data **1.75X**
	8.3 Ensure employees understand the repercussions of disclosing sensitive data **X**
	8.4 Ensure that sensitive data is adequately secured **3X**
	8.5 Ensure adequate management oversight of privacy issues **1.5X**
9. Maximize Organizational Integrity	9.1 Create an environment that empowers employees **1.5X**
	9.2 Create an environment that promotes respect **1.5X**
	9.3 Create an environment that promotes individual reliability **1.5X**
	9.4 Ensure adequate management oversight of organizational integrity issues **X**

Notes: For the upper level weights, it was previously determined that attempting to weight the 9 fundamental objectives against each other would not work. Thus, the upper level objectives were grouped in terms of similarity to make the process simpler from a conceptual basis. The following scheme was used.

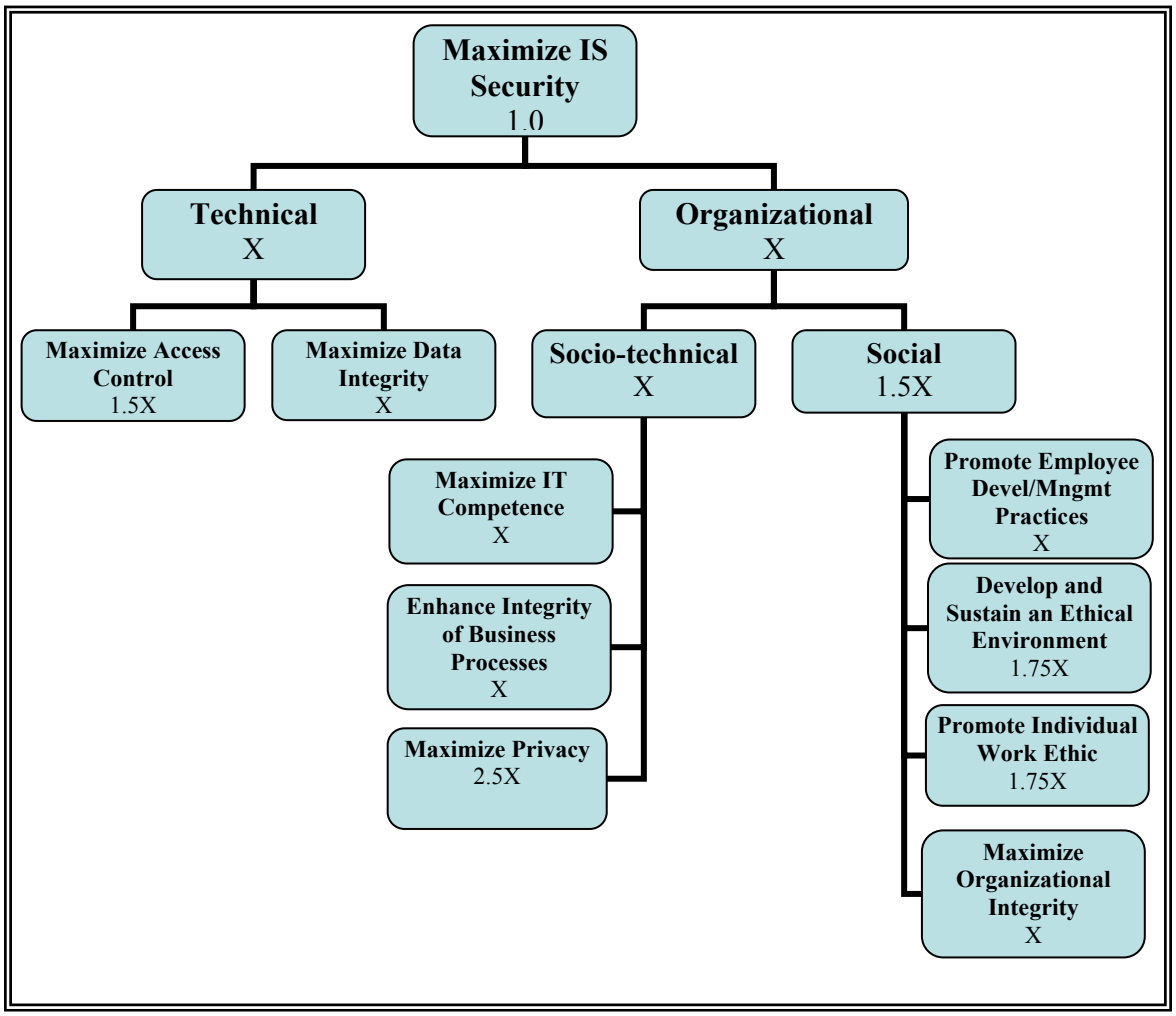

Figure B.1: Weighting Raw Data - Auditor 1

Meeting 7 - Weights

Location: Organization
Attendees: Jeffrey May, Auditor 2

Purpose: To determine weights for all of the objectives. This process was done on an individual basis for Auditor 2.

Notes: To determine weights, we first examined the second tier objectives. To determine these weights, each second tier objective for a particular fundamental objective was examined. The respondent was then asked to imagine each of these objectives at its worst possible level. The respondent was then asked to determine which objective he would like to see swing to its best possible level. After going through this process several times for each branch, we established ranks. The lowest ranked objective was then assigned a value of X and the remaining objectives were assigned multiples of X. For example, objective 1.5 below was considered to be 2 times more important than objective 1.1. After these values of X are assigned, weights can easily be determined by recognizing that the sum of the weights in an individual branch must be equal to 1. For example, for "Maximize IT competence":

$X+X+1.5X+1.75X+2X = 1$
→ $X = 1/7 = 0.138$;
→ **OBJ1.1W** = 0.138; **OBJ1.5W** = 2 * 0.138 = 0.279

Table B.12: Weighting Raw Data – Auditor 2

First Tier	Second Tier
1. Maximize IT Competence	1.1 Develop a management team that leads by example **X**
	1.2 Ensure confidence/comfort level in using computers **X**
	1.3 Ensure an adequate understanding the importance of computer technology and how it is related to the financial well-being of your organization **1.5X**
	1.4 Ensure employees have adequate IT training **1.75X**
	1.5 Ensure IT capability level of staff **2X**
2. Promote Employee Development and Management Practices	2.1 Create an environment that promotes contribution **X**
	2.2 Instill high levels of morale **X**
	2.3 Increase/maintain pride in the organization **X**
	2.4 Develop and maintain a motivated workforce **X**
3. Develop and Sustain an Ethical Environment	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing) **2.5X**
	3.2 Develop and/or make known an understood value system in the organization **2.5X**
	3.3 Create an environment that promotes organizational loyalty **X**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment **3X**
4. Maximize Access Control	4.1 Ensure personal accountability for system use **X**
	4.2 Ensure appropriate levels of user access **1.25X**
	4.3 Ensure appropriate physical security **1.25X**
	4.4 Ensure user access is based on "need to know" **1.25X**
	4.5 Ensure adequate management oversight of access control issues. **X**
5. Promote Individual Work Ethic	5.1 Maximize employee integrity in the company **2.5X**
	5.2 Create a desire to not jeopardize the reputation of the company **X**
	5.3 Create an environment that promotes the organization's best interests rather than personal gain. **X**
	5.4 Minimize temptation to use information for personal benefit **1.5X**
6. Maximize Data Integrity	6.1 Ensure that inappropriate changes to data are minimized **X**
	6.2 Ensure appropriate data integrity controls for the processing of data **X**
	6.3 Ensure adequate management oversight of data integrity issues **X**
7. Enhance Integrity of Business Processes	7.1 Ensure an understanding of the expected use of available information and its relation to individual business processes **2.25X**
	7.2 Develop procedures for managing changes to business processes **X**
	7.3 Ensure that appropriate organizational controls are in place **3X**
8. Maximize Privacy	8.1 Emphasize importance of data privacy **X**
	8.2 Ensure employee awareness against disclosure of sensitive data **1.25X**
	8.3 Ensure employees understand the repercussions of disclosing sensitive data **1.75X**
	8.4 Ensure that sensitive data is adequately secured **3X**
	8.5 Ensure adequate management oversight of privacy issues **X**
9. Maximize Organizational Integrity	9.1 Create an environment that empowers employees **X**
	9.2 Create an environment that promotes respect **X**
	9.3 Create an environment that promotes individual reliability **X**
	9.4 Ensure adequate management oversight of organizational integrity issues **X**

Notes: For the upper level weights, it was previously determined that attempting to weight the 9 fundamental objectives against each other would not work. Thus, the upper level objectives were grouped in terms of similarity to make the process simpler from a conceptual basis. The following scheme was used.

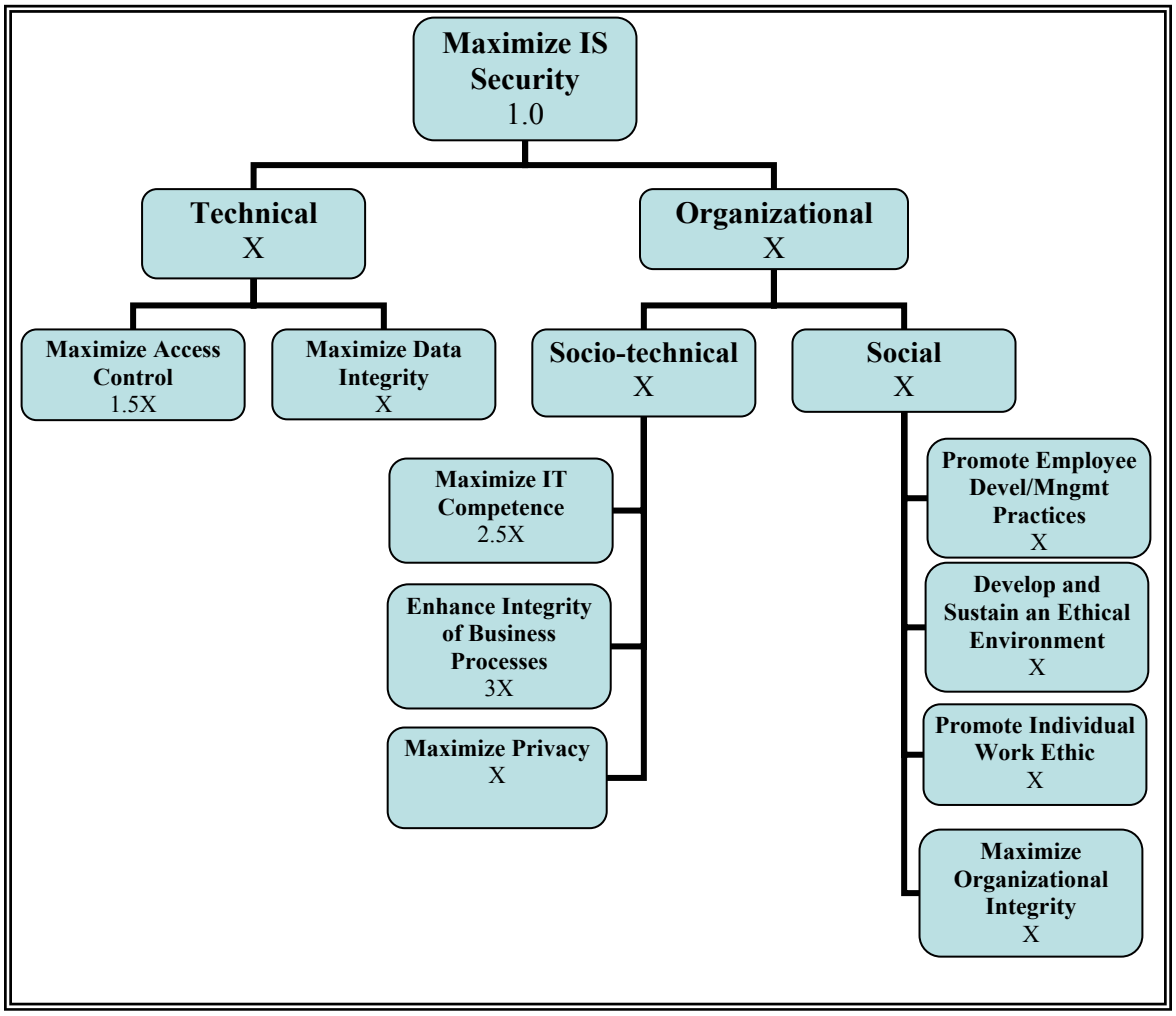

Figure B.2: Weighting Raw Data – Auditor 2

Meeting 8 – Generating Tasks

Location: Organization
Attendees: Jeffrey May, Auditor 1, Auditor 2, Auditor 3

Purpose: To determine a list of tasks that could be used to attain various second tier objectives.

NOTES:

- Each member was asked to look at the value-driven hierarchy with weights (Table 4.14, Section 4.4)
- Each member of the Team was then given a hard copy of a Task Generation List and was asked to look it over.
- Each member was asked to review the Means Objectives Hierarchy – Table 2.2.
- Each member was then asked to look at each individual objective and the various sub-objectives on a particular page. For each sub-objective each member was asked to write down as many tasks as he could think of to achieve the sub-objective.
    - Members were asked to not worry about repeating tasks. In other words, we will clean everything up later.
    - Members were asked to not worry about how strong or weak a task may be as we may remove or add tasks later.
    - Remember, this is a brainstorming exercise at this point. We are not worried about accuracy. The more things you write down, the better our group session will become.
- Each member's tasks were then collected and redundant tasks were removed.
- The following tables illustrate a first draft of the organized list of tasks.
- A finalized list of these tasks along with their various scores can be found in Section 4.5.

Table B.13: Raw Tasks for Maximize Access Control

Sub-Objective	Tasks
Maintain personal accountability for system use	• Limit the use of group accounts or generic IDs • Passwords controls (to force changes) • Unique logons • Policies and procedures
Ensure appropriate levels of user access	• Pre-defined roles and rights • Authorization procedures • Centralized system administration • Periodic management review of access • Grant access on a need to know basis
Ensure appropriate physical security	• Badges/key card (Access Controls) • Video surveillance • Security guards • Policies
Ensure user access is based on "need to know"	• Job descriptions • Pre-defined roles and rights • Policies • Segregation of duties matrix • Access monitoring systems (consolidated user rights)
Ensure adequate management oversight of access control	• Periodic review of access user access • Security administration • Secondary review of access requests • Audit log reviews • Review of termination lists (centralized review) • Established information security group • Written policies and procedures

Table B.14: Raw Tasks for Maximize Data Integrity

Sub-Objective	Tasks
Minimize inappropriate changes to data	• Access based on need to know • Authorization procedures • Audit log reviews • Edit and validation routines
Ensure appropriate data integrity controls for the processing of data	• Edit and validation routines • Reconciliations • Control totals
Ensure adequate management oversight of data integrity issues	• Error resolution process • Error log • Information Security group • Review of reconciliations and control totals

Table B.15: Raw Tasks for Maximize IT Competence

Sub-Objective	Tasks
Develop a management team that leads by example	• Written guiding principles • Written code of conduct/code of ethics • Goals • Compensation/incentive programs designed to influence appropriate decision making • Empowerment
Ensure confidence/comfort level in using computers	• Training and development • Job qualifications/descriptions that require certain skills • Standardized platforms
Create legitimate opportunities for financial gain	• Compensation programs aligned with Company values • Recognition programs • Goals and incentives tied to performance
Ensure employees have adequate IT training	• Skills assessments • Budget for training • Offer internal training • Standard platforms • Individual development plans
Ensure IT capability level of staff	• Budget for training • Skills assessment • Offer internal training • Individual development plans • Performance evaluations

Table B.16: Raw Tasks for Enhance Integrity of Business Processes

Sub-Objective	Tasks
Understand the expected use of available information and its relation to individual business processes	• Document business processes • Written requirements for systems design • Classification standards • Record retention policies
Develop procedures for managing changes to business processes	• Business process improvement program • Business process maturity/lifecycle model • Provide training on process design
Ensure that appropriate organizational controls are in place	• Risk assessment process • Documented segregation of duties matrix • Business process improvement program • Project Management Office • Executive management oversight • Steering committee

Table B.17: Raw Tasks for Maximize Privacy

Sub-Objective	Tasks
Emphasize importance of data privacy	• Security awareness program • Written code of conduct • Privacy policies • Corporate communication protocol • Document classification • Employee manual • Posters in the coffee room • Consequences for not following • Non-disclosure agreement
Ensure employee awareness against disclosure of sensitive data	• Security awareness program • Written code of conduct • Privacy policies • Corporate communication protocol • Document classification • Employee manual • Posters in the coffee room • Consequences for not following • Non-disclosure agreement
Ensure employees understand the repercussions of disclosing sensitive data	• Security awareness program • Written code of conduct • Privacy policies • Corporate communication protocol • Document classification • Employee manual • Posters in the coffee room • Public announcements of violations • Non-disclosure agreement
Ensure that sensitive data is adequately secured	• Access controls including physical controls • Classification standards • Periodic review • Audit logs • Information security policy • (See maximize access control page)
Ensure adequate management oversight of privacy issues	• Privacy policy • Privacy officer • Incident response team • Periodic review of public information • Privacy training

Table B.18: Raw Tasks for Promote Employee Development and Management Practices

Sub-Objective	Tasks
Create an environment that promotes contribution	• Rewards program • Compensation and incentives tied to performance • Guiding principles • Empower employees
Instill high levels of morale	• Teambuilding • Open communication • Adequate compensation and incentive programs • Set appropriate tone at the top • Career paths • Provide training and development programs
Increase/maintain pride in the organization	• Teambuilding • Participate in local/community events • Guiding principles • Contribution/matching program • Corporate communications function
Develop and maintain a motivated workforce	• Teambuilding • Open communication • Adequate compensation and incentive programs • Set appropriate tone at the top • Career paths • Provide training and development programs

Table B.19: Raw Tasks for Develop and Sustain an Ethical Environment

Sub-Objective	Tasks
Create an environment that makes it ok to report unethical behavior (whistle blowing)	• Hotline • Policy of no retaliation to employees who report suspected issues • Guiding principles • Written code of conduct
Instill professional-based work ethics	• Code of conduct/written ethics policy • Hiring policies • Job descriptions • Background and credit checks
Create an environment that promotes organizational loyalty	• Guiding principles • Compensation programs tied to performance • Open communication
Ensure adequate management oversight of developing and sustaining an ethical environment	• Chief Ethics Officer • Ethics Committee • Ethics reports to the board or audit committee • Written code of conduct • Periodic questionnaires of employees • Employees reaffirm policy on a periodic basis

Table B.20: Raw Tasks for Promote Individual Work Ethic

Sub-Objective	Tasks
Maximize employee integrity in the company	• Written code of conduct • Guiding principles • Management leads by example • Hiring policies including background checks
Create a desire to not jeopardize the reputation of the company	• Guiding principles • Code of conduct • Communications policy • Compensation programs tied to performance • Ethics policy • Repercussions are known if policy violated
Create an environment that promotes the organization's best interests rather than personal gain.	• Guiding principles • Code of conduct • Communications policy • Compensation programs tied to performance • Ethics policy • Repercussions are known if policy violated
Minimize temptation to use information for personal benefit	• Controls over access to data • Non-disclosure agreement with consequences • Compensation programs tied to performance • Code of Conduct • Guiding Principles

Table B.21: Raw Tasks for Maximize Organizational Integrity

Sub-Objective	Tasks
Create an environment that empowers employees	• Authority delegation (written) • Written goals and objectives • Compensation and incentives tied to performance • Appropriate levels of management
Create an environment that promotes respect	• Guiding principles • HR Policies and Procedures • Employee handbook • Open communication/Communication policy • Performance management including upward feedback
Create an environment that promotes individual reliability	• Guiding principles • Performance evaluations • Compensation program tied to performance • Open communications • Rewards program • Hiring policies and written job descriptions
Ensure adequate management oversight of organizational integrity issues	• Ethics committee • Ethics reports to the Audit Committee • Annul ethics questionnaire • Ethics policy • Guiding principles • Budget/Financial reviews • Dashboards • Communication policy • Board and Audit Committee review of business plans

Meeting 9 – Scoring Tasks

Location: Organization
Attendees: Jeffrey May, Auditor 1, Auditor 2, Auditor 3

Purpose: To score the list of tasks that relate to each second tier objective.

NOTES:

- After the tasks were organized, the next step was to score the various tasks against their appropriate evaluation measures using the evaluation measures and value functions shown in Appendix C.
- Each task received a score that ranged from the lowest to highest possible score for each evaluation measure (0.0 – 1.0).
- To determine these scores, the Team was brought together and considered each task for a particular measure before advancing to the next task.
    - In most cases, the Team arrived at a consensus for each score for the various tasks.
    - However, there were some slight discrepancies for some of the tasks, thus the average score for the three members of the Team was calculated for these cases.
- Via this process, some new tasks were determined and some of the original tasks were removed.
- A finalized list of these tasks along with their various scores can be found in Section 4.5 in Tables 4.15-4.24.

Appendix C: Evaluation Measures and Value Functions for each Second Tier Objective of the Finalized Value Hierarchy

Maximize IT Competence

Table C.1: Evaluation Measures and Value Function for "Develop a management team that leads by example"

1.1 Develop a management team that leads by example		
Evaluation Measures		
M	You or your management team attempt to develop an environment that leads by example for the purpose of encouraging IT competence.	
O	You feel that your management team attempts to develop an environment that leads by example for the purpose of encouraging IT competence.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on developing a management team that leads by example for the purpose of encouraging IT competence. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.2: Evaluation Measures and Value Function for "Increase confidence/ comfort level in using computers"

1.2 Increase confidence/comfort level in using computers		
Evaluation Measures		
M	You or your management team provides an environment that increases individual confidence/comfort level with computer technology.	
O	You feel as if your management team provides an environment that increases individual confidence/comfort level with computer technology.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on increasing the confidence/comfort level in using computers for the members of your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on increasing the confidence/ comfort level in using computers for the members of your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on increasing the confidence/ comfort level in using computers for the members of your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on increasing the confidence/comfort level in using computers for the members of your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on increasing the confidence/comfort level in using computers for the members of your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.3: Evaluation Measure and Value Function for "Ensure understanding the importance of computer technology and how it is related to the financial well-being of your organization"

1.3 Ensure an adequate understanding of the importance of computer technology and how it is related to the financial well-being of your organization		
Evaluation Measures		
M	You or your management team adequately ensures an understanding to your employees of the importance of computer technology and how it is related to the financial well-being of your organization.	
O	You understand the importance of computer technology and how it is related to the financial well-being of your organization.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that employees adequately understand the importance of computer technology and how it is related to the financial well-being of your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that employees adequately understand the importance of computer technology and how it is related to the financial well-being of your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that employees adequately understand the importance of computer technology and how it is related to the financial well-being of your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that employees adequately understand the importance of computer technology and how it is related to the financial well-being of your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that employees adequately understand the importance of computer technology and how it is related to the financial well-being of your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.4: Evaluation Measures and Value Function for "Ensure employees have adequate IT training"

1.4 Ensure employees have adequate IT training		
Evaluation Measures		
M	You or your management team provides adequate IT training opportunities.	
O	You feel as if you have adequate opportunities for IT training.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring employees in your organization have adequate IT training. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring employees in your organization have adequate IT training. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring employees in your organization have adequate IT training. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring employees in your organization have adequate IT training. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring employees in your organization have adequate IT training. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.5: Evaluation Measures and Value Function for "Ensure IT capability level of staff"

1.5 Ensure IT capability level of staff		
Evaluation Measures		
M	You or your management team ensures a proper level of IT capability amongst your staff.	
O	You feel as if you and your peers have an adequate level of IT capability.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring the IT capability level of the employees within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring the IT capability level of the employees within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring the IT capability level of the employees within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring the IT capability level of the employees within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring the IT capability level of the employees within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Promote Employee Development and Management Practices

Table C.6: Evaluation Measures and Value Function for "Create an environment that promotes contribution"

2.1 Create an environment that promotes contribution		
Evaluation Measures		
M	You or your management team creates an environment where your subordinates desire to contribute.	
O	You feel as if you work in an environment that promotes contribution.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that promotes contribution within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that promotes contribution within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that promotes contribution within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that promotes contribution within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that promotes contribution within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.7: Evaluation Measures and Value Function for "Instill high levels of morale"

2.2 Instill high levels of morale		
Evaluation Measures		
M	You or your management team creates an environment that instills high levels of morale.	
O	You feel as if you work in an environment that instills high levels of morale.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that instills high levels of morale within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that instills high levels of morale within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that instills high levels of morale within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that instills high levels of morale within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that instills high levels of morale within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.8: Evaluation Measures and Value Function for "Increase/maintain pride in the organization"

2.3 Increase/maintain pride in the organization		
Evaluation Measures		
M	You or your management team creates an environment that increases/maintains pride in the organization.	
O	You feel you work in an environment that increases/maintains pride in the organization.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that increases/ maintains pride in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that increases/maintains pride in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that increases/maintains pride in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that increases/maintains pride in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that increases/maintains pride in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.9: Evaluation Measures and Value Function for "Develop and maintain a motivated workforce"

2.4 Develop and maintain a motivated workforce		
Evaluation Measures		
M	You or your management team creates an environment that develops and maintains a motivated workforce.	
O	You feel you work in an environment that develops and maintains a motivated workforce.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that develops and maintains a motivated workforce in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that develops and maintains a motivated workforce in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that develops and maintains a motivated workforce in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that develops and maintains a motivated workforce in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that develops and maintains a motivated workforce in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Develop and Sustain an Ethical Environment

Table C.10: Evaluation Measures and Value Function for "Create an environment that makes it ok to report unethical behavior (whistle blowing)"

3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)		
Evaluation Measures		
M	You or your management team creates an environment that makes it ok to report unethical behavior (whistle blowing).	
O	You feel that you have been made aware of the importance of reporting unethical behavior.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that makes it ok to report unethical behavior (whistle blowing) in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that makes it ok to report unethical behavior (whistle blowing) in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that makes it ok to report unethical behavior (whistle blowing) in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that makes it ok to report unethical behavior (whistle blowing) in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that makes it ok to report unethical behavior (whistle blowing) in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.11: Evaluation Measures and Value Function for "Develop and/or make known an understood value system in the organization"

3.2 Develop and/or make known an understood value system in the organization		
Evaluation Measures		
M	You or your management team has developed and/or made known a well-defined value system to your employees.	
O	You feel that you understand the value system of your organization.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on developing and/or making known an understood value system within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on developing and/or making known an understood value system within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on developing and/or making known an understood value system within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on developing and/or making known an understood value system within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on developing and/or making known an understood value system within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.12: Evaluation Measures and Value Function for "Create an environment that promotes organizational loyalty"

3.3 Create an environment that promotes organizational loyalty		
Evaluation Measures		
M	You or your management team creates an environment that promotes organizational loyalty.	
O	You feel you work in an environment that promotes organizational loyalty.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that promotes organizational loyalty within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that promotes organizational loyalty within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that promotes organizational loyalty within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that promotes organizational loyalty within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that promotes organizational loyalty within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.13: Evaluation Measure and Value Function for "Ensure adequate management oversight of developing and sustaining an ethical environment"

3.4 Ensure adequate management oversight of developing and sustaining an ethical environment		
Evaluation Measures		
MO	You feel that your organization ensures adequate management oversight of developing and sustaining an ethical environment.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring adequate management oversight of developing and sustaining an ethical environment within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring adequate management oversight of developing and sustaining an ethical environment within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring adequate management oversight of developing and sustaining an ethical environment within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring adequate management oversight of developing and sustaining an ethical environment within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring adequate management oversight of developing and sustaining an ethical environment within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Maximize Access Control

Table C.14: Evaluation Measure and Value Function for "Ensure personal accountability for system use"

4.1 Ensure personal accountability for system use		
Evaluation Measures		
M	You or your management team ensures that personal accountability for access control is maintained at adequate levels.	
O	You feel as if personal accountability for access control is maintained at adequate levels.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that personal accountability for access control within your organization is maintained at adequate levels. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that personal accountability for access control within your organization is maintained at adequate levels. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that personal accountability for access control within your organization is maintained at adequate levels. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that personal accountability for access control within your organization is maintained at adequate levels. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that personal accountability for access control within your organization is maintained at adequate levels. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.15: Evaluation Measure and Value Function for "Ensure appropriate levels of user access"

4.2 Ensure appropriate levels of user access		
Evaluation Measures		
M	You or your management team ensures the appropriate levels of user access to pertinent data for your employees.	
O	You feel that your organization provides you with the appropriate levels of user access to pertinent data.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring the appropriate levels of user access to pertinent data to your employees within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring the appropriate levels of user access to pertinent data to your employees within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring the appropriate levels of user access to pertinent data to your employees within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring the appropriate levels of user access to pertinent data to your employees within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring the appropriate levels of user access to pertinent data to your employees within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.16: Evaluation Measure and Value Function for "Ensure appropriate physical security"

4.3 Ensure appropriate physical security		
Evaluation Measures		
M	You or your management team ensures the appropriate levels of physical security for technology within your organization.	
O	You feel that the technology within your organization is physically secure at an appropriate level.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring the appropriate levels of physical security for technology within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring the appropriate levels of physical security for technology within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring the appropriate levels of physical security for technology within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring the appropriate levels of physical security for technology within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring the appropriate levels of physical security for technology within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.17: Evaluation Measure and Value Function for "Ensure user access is based on "need to know""

4.4 Ensure user access is based on "need to know"		
Evaluation Measures		
M	You or your management team ensures that user access is established on a "need to know" basis within your organization.	
O	You are not able to access sensitive data that is not pertinent to your job.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that user access is established on a "need to know" basis to the employees within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that user access is established on a "need to know" basis to the employees within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that user access is established on a "need to know" basis to the employees within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that user access is established on a "need to know" basis to the employees within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that user access is established on a "need to know" basis to the employees within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.18: Evaluation Measure and Value Function for "Ensure adequate management oversight of access control issues"

4.5 Ensure adequate management oversight of access control issues		
Evaluation Measures		
MO	You feel that your organization ensures adequate management oversight of access control issues.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring adequate management oversight of access control issues within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring adequate management oversight of access control issues within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring adequate management oversight of access control issues within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring adequate management oversight of access control issues within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring adequate management oversight of access control issues within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Promote Individual Work Ethic

Table C.19: Evaluation Measures and Value Function for "Maximize employee integrity in the company"

5.1 Maximize employee integrity in the company		
Evaluation Measures		
M	You or your management team attempt to create an environment that maximizes employee integrity in the organization.	
O	You feel as if you work in an environment that emphasizes employee integrity in the organization.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that maximizes employee integrity in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that maximizes employee integrity in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that maximizes employee integrity in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that maximizes employee integrity in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that maximizes employee integrity in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.20: Evaluation Measures and Value Function for "Minimize urgency of personal gain"

5.2 Minimize urgency of personal gain		
Evaluation Measures		
M	You or your management team attempt to create an environment that minimizes the urgency of personal gain.	
O	You feel as if you work in an environment that minimizes the urgency of personal gain.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that minimizes the urgency of personal gain in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that minimizes the urgency of personal gain in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that minimizes the urgency of personal gain in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that minimizes the urgency of personal gain in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that minimizes the urgency of personal gain in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.21: Evaluation Measures and Value Function for "Create a desire to not jeopardize the position of the company"

5.3 Create a desire to not jeopardize the position of the company		
Evaluation Measures		
M	You or your management team attempt to create an environment that promotes a desire to not jeopardize the position of the company.	
O	You feel as if you work in an environment that promotes a desire to not jeopardize the position of the company.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that promotes a desire to not jeopardize the position of the company in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that promotes a desire to not jeopardize the position of the company in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that promotes a desire to not jeopardize the position of the company in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that promotes a desire to not jeopardize the position of the company in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that promotes a desire to not jeopardize the position of the company in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.22: Evaluation Measures and Value Function for "Create an environment that promotes company profitability rather than personal gain"

5.4 Create an environment that promotes company profitability rather than personal gain		
Evaluation Measures		
M	You or your management team attempt to create an environment that promotes company profitability rather than personal gain.	
O	You feel as if you work in an environment that promotes company profitability rather than personal gain.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that promotes company profitability rather than personal gain in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that promotes company profitability rather than personal gain in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that promotes company profitability rather than personal gain in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that promotes company profitability rather than personal gain in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that promotes company profitability rather than personal gain in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.23: Evaluation Measures and Value Function for "Minimize temptation to use information for personal benefit"

5.5 Minimize temptation to use information for personal benefit		
Evaluation Measures		
M	You or your management team creates an environment that minimizes the temptation of your employees to use information for personal benefit.	
O	You feel as if you work in an environment that minimizes the temptation for you to use information for personal benefit beyond what is required for your job.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that minimizes the temptation of the employees within your organization to use information for personal benefit. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that minimizes the temptation of the employees within your organization to use information for personal benefit. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that minimizes the temptation of the employees within your organization to use information for personal benefit. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that minimizes the temptation of the employees within your organization to use information for personal benefit. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that minimizes the temptation of the employees within your organization to use information for personal benefit. Impacts will definitely be realized by both management and operational employees.	**1**

Maximize Data Integrity

Table C.24: Evaluation Measures and Value Function for "Ensure that inappropriate changes to data are minimized"

6.1 Ensure that inappropriate changes to data are minimized		
Evaluation Measures		
M	You or your management team ensures that inappropriate changes to sensitive data are minimized.	
O	You feel as if the sensitive data in your organization is adequately protected against inappropriate changes.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that inappropriate changes to data are minimized within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that inappropriate changes to data are minimized within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that inappropriate changes to data are minimized within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that inappropriate changes to data are minimized within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that inappropriate changes to data are minimized within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.25: Evaluation Measure and Value Function for "Ensure appropriate data integrity controls for the processing of data"

6.2 Ensure appropriate data integrity controls for the processing of data		
Evaluation Measures		
M	You or your management team ensures that appropriate data integrity controls for the processing of data is present in your organization.	
O	You feel as if adequate controls for the purpose of maintaining the integrity of pertinent data within your organization have been established.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that appropriate data integrity controls for the processing of data is present within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that appropriate data integrity controls for the processing of data is present within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that appropriate data integrity controls for the processing of data is present within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that appropriate data integrity controls for the processing of data is present within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that appropriate data integrity controls for the processing of data is present within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.26: Evaluation Measure and Value Function for "Ensure adequate management oversight of data integrity issues"

6.3 Ensure adequate management oversight of date integrity issues		
Evaluation Measures		
MO	You feel that your organization ensures adequate management oversight of data integrity issues.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring adequate management oversight of data integrity issues within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring adequate management oversight of data integrity issues within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring adequate management oversight of data integrity issues within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring adequate management oversight of data integrity issues within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring adequate management oversight of data integrity issues within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Enhance Integrity of Business Processes

Table C.27: Evaluation Measures and Value Function for "Ensure an understanding of the expected use of available information and its relation to individual business processes"

7.1 Ensure an understanding of the expected use of available information and its relation to individual business processes		
Evaluation Measures		
M	You or your management team ensures that employees understand the expected use of information and its relation to individual business processes.	
O	You feel as if you understand the expected use of available information and its relation to individual business processes	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that employees in your organization understand the expected use of information and its relation to individual business processes. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that employees in your organization understand the expected use of information and its relation to individual business processes. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that employees in your organization understand the expected use of information and its relation to individual business processes. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that employees in your organization understand the expected use of information and its relation to individual business processes. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that employees in your organization understand the expected use of information and its relation to individual business processes. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.28: Evaluation Measures and Value Function for "Develop procedures for managing changes to business processes"

7.2 Develop procedures for managing changes to business processes		
Evaluation Measures		
M	You or your management team are aware of or take part in developing procedures for managing changes to business processes.	
O	You feel as if you understand the procedures required for changing business processes.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on developing procedures for managing changes to business processes in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on developing procedures for managing changes to business processes in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on developing procedures for managing changes to business processes in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on developing procedures for managing changes to business processes in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on developing procedures for managing changes to business processes in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.29: Evaluation Measures and Value Function for "Ensure that appropriate organizational controls are in place"

7.3 Ensure that appropriate organizational controls are in place		
Evaluation Measures		
M	You or your management team have developed appropriate organizational controls of business processes and made them understandable to your employees.	
O	You feel as if you have an accurate understanding of business process controls set forth by your organization.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on developing appropriate organizational controls of business processes and making them understandable to the employees in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on developing appropriate organizational controls of business processes and making them understandable to the employees in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on developing appropriate organizational controls of business processes and making them understandable to the employees in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on developing appropriate organizational controls of business processes and making them understandable to the employees in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on developing appropriate organizational controls of business processes and making them understandable to the employees in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Maximize Privacy

Table C.30: Evaluation Measures and Value Function for "Emphasize importance of data privacy"

8.1 Emphasize importance of data privacy		
Evaluation Measures		
M	You or your management team emphasizes the importance of data privacy to your employees.	
O	You feel as if your organization has emphasized the importance of data privacy.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on emphasizing the importance of data privacy to the employees in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on emphasizing the importance of data privacy to the employees in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on emphasizing the importance of data privacy to the employees in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on emphasizing the importance of data privacy to the employees in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on emphasizing the importance of data privacy to the employees in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.31: Evaluation Measures and Value Function for "Ensure employee awareness against disclosure of sensitive data"

8.2 Ensure employee awareness against disclosure of sensitive data		
Evaluation Measures		
M	You or your management team emphasizes the importance of rules against unethical or unlawful disclosure of sensitive data.	
O	You feel as if your organization has emphasized the importance of rules against unethical or unlawful disclosure of sensitive data.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on emphasizing the importance of rules against unethical or unlawful disclosure of sensitive data to the employees in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on emphasizing the importance of rules against unethical or unlawful disclosure of sensitive data to the employees in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on emphasizing the importance of rules against unethical or unlawful disclosure of sensitive data to the employees in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on emphasizing the importance of rules against unethical or unlawful disclosure of sensitive data to the employees in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on emphasizing the importance of rules against unethical or unlawful disclosure of sensitive data to the employees in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.32: Evaluation Measures and Value Function for "Ensure employees understand the repercussions of disclosing sensitive data"

8.3 Ensure employees understand the repercussions of disclosing sensitive data		
Evaluation Measures		
M	You or your management team ensures that employees understand the repercussions of disclosing sensitive data.	
O	You feel as if your organization has emphasized the repercussions of disclosing sensitive data.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that employees in your organization understand the repercussions of disclosing sensitive data. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that employees in your organization understand the repercussions of disclosing sensitive data. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that employees in your organization understand the repercussions of disclosing sensitive data. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that employees in your organization understand the repercussions of disclosing sensitive data. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that employees in your organization understand the repercussions of disclosing sensitive data. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.33: Evaluation Measures and Value Function for "Ensure that sensitive data is adequately secured"

8.4 Ensure that sensitive data is adequately secured		
Evaluation Measures		
M	You or your management team ensures that sensitive data is adequately secured.	
O	You feel as if your organization ensures that sensitive data is adequately secured.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring that sensitive data is adequately secured in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring that sensitive data is adequately secured in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring that sensitive data is adequately secured in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring that sensitive data is adequately secured in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring that sensitive data is adequately secured in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.34: Evaluation Measures and Value Function for "Ensure adequate management oversight of privacy issues"

8.5 Ensure adequate management oversight of privacy issues		
Evaluation Measures		
MO	You feel that your organization ensures adequate management oversight of privacy issues.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring adequate management oversight of privacy issues within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring adequate management oversight of privacy issues within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring adequate management oversight of privacy issues within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring adequate management oversight of privacy issues within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring adequate management oversight of privacy issues within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Maximize Organizational Integrity

Table C.35: Evaluation Measures and Value Function for "Create an environment that empowers employees"

9.1 Create an environment that empowers employees		
Evaluation Measures		
M	You or your management team creates an environment that empowers employees.	
O	You feel as if you work in an environment that empowers you to do what it takes to get the job done.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that empowers employees in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that empowers employees in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that empowers employees in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that empowers employees in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that empowers employees in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.36: Evaluation Measures and Value Function for "Create an environment that promotes respect"

9.2 Create an environment that promotes respect		
Evaluation Measures		
M	You or your management team creates an environment that promotes respect.	
O	You feel as if you work in an environment that promotes respect amongst you and your co-workers.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that promotes respect amongst the employees in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that promotes respect amongst the employees in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that promotes respect amongst the employees in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that promotes respect amongst the employees in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that promotes respect amongst the employees in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.37: Evaluation Measures and Value Function for "Create an environment that promotes individual reliability"

9.3 Create an environment that promotes individual reliability		
Evaluation Measures		
M	You or your management team creates an environment that promotes individual reliability.	
O	You feel as if you work in an environment that promotes individual reliability.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on creating an environment that promotes individual reliability of the employees in your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on creating an environment that promotes individual reliability of the employees in your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on creating an environment that promotes individual reliability of the employees in your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on creating an environment that promotes individual reliability of the employees in your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on creating an environment that promotes individual reliability of the employees in your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Table C.38: Evaluation Measures and Value Function for "Ensure adequate management oversight of organizational integrity issues"

9.4 Ensure adequate management oversight of organizational integrity issues		
Evaluation Measures		
MO	You feel that your organization ensures adequate management oversight of organizational integrity issues.	
Value Function		
Point	**Definition**	**Value**
Not at All	If this task is implemented to the best of its ability, it has no impact on ensuring adequate management oversight of organizational integrity issues within your organization. Impacts will not be realized by either management or operational employees.	**0**
Limited	If this task is implemented to the best of its ability, it has a very subtle impact on ensuring adequate management oversight of organizational integrity issues within your organization. Impacts might be realized by either management or operational employees.	**0.3**
Somewhat	If this task is implemented to the best of its ability, it has somewhat of an impact on ensuring adequate management oversight of organizational integrity issues within your organization. Impacts could be realized by either management or operational employees.	**0.5**
Mostly	If this task is implemented to the best of its ability, it has a strong but not overwhelming impact on ensuring adequate management oversight of organizational integrity issues within your organization. Impacts might be realized by both management and operational employees.	**0.7**
Direct	If this task is implemented to the best of its ability, it will have an overwhelming impact on ensuring adequate management oversight of organizational integrity issues within your organization. Impacts will definitely be realized by both management and operational employees.	**1**

Appendix D: Description of Duties for Respondents

Description of Duties for Auditor 1:

TITLE: General Auditor - FINANCE GROUP

PURPOSE
Leads the corporate audit, quality assurance, and agent services functions. Directs the development and execution of a comprehensive, enterprise-wide audit plan and program and oversees the review of independent agents to mitigate associated risk. Reports to the Audit Committee of the Board of Directors, with dotted line reporting to the General Counsel.

DUTIES AND RESPONSIBILITIES
1. Initiates, cultivates and maintains professional relationships with the Board of Directors, Audit Committee, external auditors, and all levels of management.
2. Develops and executes an internal audit plan, based on risk assessment, to analyze the quality and effectiveness of internal operating policies, administrative procedures, and systems of internal control.
3. Directs staff in the preparation of audit reports, results reviews, findings, conclusions, and recommendations, including monitoring implementation.
4. Leads team assisting in internal investigations and supporting compliance efforts.
5. Ensures the effective evaluation of control areas of new systems and services prior to implementation or installation.
6. Provides audit assistance to the independent accounting firm during annual audit of financial statements.
7. Coordinates Risk Committee meetings.
8. Develops and executes a comprehensive program of quality assurance reviews of independent agents to mitigate risk.
9. Manages agent services escrow reconciliation.
10. Manages a large decentralized national staff with a focus on superior service and staff development to address complex needs of fast growing company. Maintains and promotes positive employee relations in work environment.
11. Ensures staff is provided regular training and educational updates of rules, regulations, standards and best practices in the field of internal audit and related matters of importance to the department.
12. Develops, documents, and implements policies and procedures for the Internal Audit and Quality Assurance Departments.
13. Prepares, secures approval, and implements department operating budget and operates within those guidelines.
14. Oversees audit-related due diligence for potential acquisitions.

Description of Duties for Auditor 2:

TITLE: Audit Manager-Information Systems – FINANCE GROUP

PURPOSE

Assist the Director of Internal Audit with management of the corporate audit function, including development and execution of the comprehensive risk-based audit plan designed to provide assessments of internal control processes and operational performance and facilitate the formulation of business strategies and management of risk of the information systems business segment. Plans, coordinates, directs and/or executes corporate audit projects with specific responsibility for the continuous review of all information systems, telecommunications and data processing activities. Assists with the development and maintenance of a highly professional audit staff and manages subordinate staff and staff assigned to specific projects.

ESSENTIAL DUTIES AND RESPONSIBILITIES

1. Assists in the design, development and maintenance of a comprehensive corporate audit plan of the information systems business based upon risk assessment, management's goals and objectives, and the requirements of the Board Audit Committee. Identifies potential audit areas, assesses the degree of inherent risk, proposes the level and frequency of audit coverage, and estimates the time and skills required to complete audit projects.
2. Assists the Director of Internal Audit in defining, developing, and preparing the annual audit plans, budgets and schedules.
3. Directs and/or performs systems-related audits of the Corporation in accordance with Generally Accepted Auditing Standards (as set forth by the AICPA) and the Standards for the Professional Practice of Internal Audit (as set forth by the IIA).
4. Reviews or prepares detailed plans for performing individual system-related audits including objectives, procedures, budgets and schedules.
5. Manages the activities of assigned audit team members by clarifying audit objectives, approving individual procedures, interpreting policy, and assisting in the resolution of unusual technical problems.
6. Leads the presentation and review of audit findings with key members of operating management. Recommends and explores task courses of action for correcting control weaknesses, resolving operating problems or improving performance.
7. Analyzes all actions initiated or proposed in response to audit recommendations. Monitors the completion of corrective actions and, as necessary, advises management of non-compliance.
8. Prepares or reviews and edits draft audit reports designed to provide operating and Corporate management and the Board Audit Committee with an objective assessment of systems, processes and operations and management's planned corrective actions. Ensures the results of evaluations are presented in business rather than technical terms in order to promote understanding by non-technical personnel.

Description of Duties for Auditor 3:

TITLE: Auditor Senior-Information Systems – FINANCE GROUP

PURPOSE

Under general direction of the Internal Audit Manager – Information Systems, performs or directs various auditing tasks of complex application systems in production or under development for controls and security in accordance with prescribed company policies and procedures. This is a non-supervisory position but the incumbent will lead the activities of others on an ad hoc basis, will share expertise and provide training to other members of internal audit staff, and will provide input into staff evaluations.

DUTIES AND RESPONSIBILITIES

1. Performs or directs systems audits in a professional manner, in accordance with the professional practice of Internal Audit and the Internal Audit departments risk assessment.
2. Prepares, documents, and executes computer programs in support of financial and operational audits.
3. Reviews application, relational database management system, operating system, and communication systems security to ensure access is properly controlled.
4. Reviews data center operations for both efficiency and effectiveness of processes.
5. Participates and/or leads development activity to assure that standards and controls are included in projects.
6. Provides input for revision of audit programs where necessary to accomplish audit objective.
7. Prepares audit work papers documenting each audit step in the audit program. Ensures that information is presented clearly, concisely, accurately, in logical format, timely, and in accordance with standards.
8. Makes or leads others in making oral and written presentations to management during and at conclusion of an audit, discussing deficiencies, recommending corrective action and suggesting improvements in internal controls.
9. Interview persons in area under audit to gain understanding of how the system of internal control operates.
10. Performs transaction and compliance testing to evaluate the existence, efficiency and effectiveness of internal control procedures.
11. Performs system design, development, maintenance, and support of auditing applications.
12. Assists external auditors by preparing work papers and schedules.
13. Maintains updated knowledge of rules, regulations and standards in the fields of systems internal audit and accounting and related matters of interest to the department.
14. Provides “first line” of support for hardware/software used by operational /financial auditors.

Appendix E: Deterministic Analysis

Calculations and Final Scores for the 69 Value-driven Tasks

Table E.1: Calculations and Final Scores for the 69 Value-driven Tasks

Task	Impacts Sub-Objective	Score $v_i(x_i)$	Global Weight (w_i)	Final Score $\Sigma w_i * v_i(x_i)$
T1 – Security Awareness Training	4.1 Maintain personal accountability for system use	0.7	0.0378	**0.38587**
	4.2 Ensure appropriate levels of user access	0.7	0.0517	
	4.3 Ensure appropriate physical security	0.5	0.056	
	4.4 Ensure user access is based on "need to know"	0.7	0.0517	
	4.5 Ensure adequate management oversight of access control	0.7	0.0378	
	5.4 Minimize temptation to use information for personal benefit	0.7	0.0195	
	6.1 Minimize inappropriate changes to data	0.7	0.1031	
	6.2 Ensure appropriate data integrity controls for the processing of data	0.5	0.0883	
	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.0736	
	8.1 Emphasize importance of data privacy	0.7	0.013	
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0142	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0134	
	8.4 Ensure that sensitive data is adequately secured	0.5	0.0288	
	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0118	
T2 – Limit the use of group accounts or generic IDs	4.1 Maintain personal accountability for system use	0.5	0.0378	**0.05457**
	4.2 Ensure appropriate levels of user access	0.3	0.0517	
	8.4 Ensure that sensitive data is adequately secured	0.7	0.0288	

T3 - Password controls to force unique logons	4.1 Maintain personal accountability for system use	0.7	0.0378	**0.04662**
	8.4 Ensure that sensitive data is adequately secured	0.7	0.0288	
T4 - Pre-defined roles and rights	4.4 Ensure user access is based on "need to know"	0.5	0.0517	**0.12799**
	6.1 Minimize inappropriate changes to data	0.5	0.1031	
	4.2 Ensure appropriate levels of user access	0.7	0.0517	
	8.4 Ensure that sensitive data is adequately secured	0.5	0.0288	
T5 - Authorization procedures	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195	**0.13827**
	6.1 Minimize inappropriate changes to data	0.7	0.1031	
	8.4 Ensure that sensitive data is adequately secured	0.7	0.0288	
	4.2 Ensure appropriate levels of user access	0.7	0.0517	
T6- Centralized system administration	4.2 Ensure appropriate levels of user access	0.5	0.0517	**0.04889**
	8.4 Ensure that sensitive data is adequately secured	0.8	0.0288	
T7 – Badges/key cards	4.3 Ensure appropriate physical security	0.7	0.056	**0.05936**
	8.4 Ensure that sensitive data is adequately secured	0.7	0.0288	
T8 - Video surveillance	4.3 Ensure appropriate physical security	0.5	0.056	**0.04816**
	8.4 Ensure that sensitive data is adequately secured	0.7	0.0288	
T9 - Security guards	4.3 Ensure appropriate physical security	0.7	0.056	**0.05936**
	8.4 Ensure that sensitive data is adequately secured	0.7	0.0288	
T10 – Well-defined job descriptions	4.4 Ensure user access is based on "need to know"	0.5	0.0517	**0.07740**
	6.1 Minimize inappropriate changes to data	0.5	0.1031	
T11 – Segregation of duties matrix	4.4 Ensure user access is based on "need to know"	0.5	0.0517	**0.07740**
	6.1 Minimize inappropriate changes to data	0.5	0.1031	
T12 - Automated access monitoring system	4.4 Ensure user access is based on "need to know"	0.7	0.0517	**0.10836**
	6.1 Minimize inappropriate changes to data	0.7	0.1031	

T13 - Periodic review of user access roles and rights	4.5 Ensure adequate management oversight of access control	0.7	0.0378	**0.02646**
T14 - Security administration group/policy makers	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0118	**0.08624**
	4.5 Ensure adequate management oversight of access control	0.7	0.0378	
	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.0736	
T15 – Audit log reviews	4.5 Ensure adequate management oversight of access control	0.5	0.0378	**0.0189**
T16 - Review of termination lists (centralized review)	4.5 Ensure adequate management oversight of access control	0.5	0.0378	**0.0189**
T17 - Edit and validation routines	6.2 Ensure appropriate data integrity controls for the processing of data	0.8	0.0883	**0.07064**
T18 – Reconciliation procedures	6.2 Ensure appropriate data integrity controls for the processing of data	0.7	0.0883	**0.06181**
T19 – Periodic error log audits	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.0736	**0.05152**
T20 – Periodic review of reconciliations	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.0736	**0.05152**

T21-Amendments to Guiding Principles	1.1 Develop a management team that leads by example	0.5	0.0094	**0.15826**
	2.1 Create an environment that promotes contribution	0.5	0.0149	
	2.2 Instill high levels of morale	0.7	0.0149	
	2.3 Increase/maintain pride in the organization	0.7	0.0149	
	2.4 Develop and maintain a motivated workforce	0.5	0.0149	
	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.5	0.0161	
	3.2 Instill professional-based work ethics	0.7	0.0265	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0121	
	5.1 Maximize employee integrity in the company	0.5	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195	
	8.1 Emphasize importance of data privacy	0.5	0.013	
	8.2 Ensure employee awareness against disclosure of sensitive data	0.5	0.0142	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.5	0.0134	
	9.1 Create an environment that empowers employees	0.5	0.0155	
	9.2 Create an environment that promotes respect	0.7	0.0155	
	9.3 Create an environment that promotes individual reliability	0.3	0.0155	

T22 - Amendments to Code of Business Conduct and Ethics	1.1 Develop a management team that leads by example	0.7	0.0094	**0.11501**
	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.6	0.0161	
	3.2 Instill professional-based work ethics	0.5	0.0265	
	5.1 Maximize employee integrity in the company	0.5	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195	
	8.1 Emphasize importance of data privacy	0.7	0.013	
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0142	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0134	
	9.2 Create an environment that promotes respect	0.7	0.0155	
	9.3 Create an environment that promotes individual reliability	0.3	0.0155	
T23 - Written in Job Descriptions	1.1 Develop a management team that leads by example	0.7	0.0094	**0.00658**
T24 - Compensation/ incentive programs designed to influence management teams leading by example	1.1 Develop a management team that leads by example	0.7	0.0094	**0.00658**
T25 - Empowerment Training	1.1 Develop a management team that leads by example	0.7	0.0094	**0.00658**
T26 - IT Training and development	1.2 Ensure confidence/comfort level in using computers	0.7	0.0094	**0.03220**
	1.4 Ensure employees have adequate IT training	0.7	0.0153	
	1.5 Ensure IT capability level of staff	0.7	0.0213	

T27 – Hire employees with adequate IT skills	1.2 Ensure confidence/comfort level in using computers	0.5	0.0094	**0.01535**
	1.5 Ensure IT capability level of staff	0.5	0.0213	
T28 - Standardized computer platforms	1.2 Ensure confidence/comfort level in using computers	0.5	0.0094	**0.00470**
T29 - Compensation programs aligned with company values	1.3 Create legitimate opportunities for financial gain	0.8	0.0118	**0.00944**
T30 - Recognition programs	1.3 Create legitimate opportunities for financial gain	0.3	0.0118	**0.00354**
T31 - Goals and incentives tied to job descriptions and performance	1.3 Create legitimate opportunities for financial gain	0.7	0.0118	**0.00826**
T32 - Skills assessments and performance evaluations	1.4 Ensure employees have adequate IT training	0.5	0.0153	**0.02469**
	1.5 Ensure IT capability level of staff	0.8	0.0213	
T33 - Individual development plans	1.4 Ensure employees have adequate IT training	0.7	0.0153	**0.02562**
	1.5 Ensure IT capability level of staff	0.7	0.0213	
T34 - Budget for Training	1.4 Ensure employees have adequate IT training	0.7	0.0153	**0.01071**
T35 - Process design training	7.1 Understand the expected use of available information and its relation to individual business processes	0.7	0.0736	**0.08652**
	7.3 Ensure that appropriate organizational controls are in place	0.7	0.0354	
	7.2 Develop procedures for managing changes to business processes	0.7	0.0146	
T36 - Document and make known business processes	7.1 Understand the expected use of available information and its relation to individual business processes	0.5	0.0736	**0.03680**

T37 -Create and make known information classification standards	7.1 Understand the expected use of available information and its relation to individual business processes	0.5	0.0736	**0.03680**
T38 - Create and manage a business process improvement program	7.2 Develop procedures for managing changes to business processes	0.7	0.0146	**0.01022**
T39 - Create and adhere to business process maturity/lifecycle model	7.2 Develop procedures for managing changes to business processes	0.7	0.0146	**0.01022**
T40 - Risk assessment activities	7.3 Ensure that appropriate organizational controls are in place	0.7	0.0354	**0.02478**
T41 - Periodic review of business process improvement program	7.3 Ensure that appropriate organizational controls are in place	0.7	0.0354	**0.02478**
T42 - Executive management oversight	7.3 Ensure that appropriate organizational controls are in place	0.7	0.0354	**0.02478**
T43 - Amendments to Employee Manual	8.1 Emphasize importance of data privacy	0.7	0.013	**0.02842**
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0142	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0134	
T44 - Posters in the coffee room	8.2 Ensure employee awareness against disclosure of sensitive data	0.5	0.0142	**0.02030**
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.5	0.0134	
	8.1 Emphasize importance of data privacy	0.5	0.013	

T45 – Nondisclosure agreement with repercussions	5.2 Create a desire to not jeopardize the reputation of the company	0.7	0.013	**0.05669**
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013	
	5.4 Minimize temptation to use information for personal benefit	0.7	0.0195	
	8.2 Ensure employee awareness against disclosure of sensitive data	0.9	0.0142	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.9	0.0134	
T46 - Privacy officer	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0118	**0.00826**
T47 - Incident response team	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0118	**0.00826**
T48 - Periodic review of public information	8.5 Ensure adequate management oversight of privacy issues	0.5	0.0118	**0.00590**
T49 - Oversee Privacy aspects of Security Awareness Training	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0118	**0.00826**
T50 - Authority delegation (written document for empowerment)	2.1 Create an environment that promotes contribution	0.9	0.0149	**0.09830**
	2.2 Instill high levels of morale	0.9	0.0149	
	2.3 Increase/maintain pride in the organization	0.7	0.0149	
	2.4 Develop and maintain a motivated workforce	0.5	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0121	
	5.1 Maximize employee integrity in the company	0.5	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013	
	9.1 Create an environment that empowers employees	0.9	0.0155	
	9.2 Create an environment that promotes respect	0.7	0.0155	

T51 - Compensation and incentives tied to performance	2.1 Create an environment that promotes contribution	0.9	0.0149	**0.11343**
	2.2 Instill high levels of morale	0.8	0.0149	
	2.3 Increase/maintain pride in the organization	0.7	0.0149	
	2.4 Develop and maintain a motivated workforce	0.5	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.7	0.0121	
	5.1 Maximize employee integrity in the company	0.5	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195	
	9.1 Create an environment that empowers employees	0.7	0.0155	
	9.3 Create an environment that promotes individual reliability	0.6	0.0155	
T52 - Rewards program tied to employee performance	2.1 Create an environment that promotes contribution	0.7	0.0149	**0.10776**
	2.2 Instill high levels of morale	0.8	0.0149	
	2.3 Increase/maintain pride in the organization	0.7	0.0149	
	2.4 Develop and maintain a motivated workforce	0.9	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.7	0.0121	
	5.1 Maximize employee integrity in the company	0.7	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.7	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.8	0.013	
	9.3 Create an environment that promotes individual reliability	0.7	0.0155	

T53 – Well-defined career paths	2.1 Create an environment that promotes contribution	0.5	0.0149	**0.08743**
	2.2 Instill high levels of morale	0.7	0.0149	
	2.3 Increase/maintain pride in the organization	0.5	0.0149	
	2.4 Develop and maintain a motivated workforce	0.8	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.3	0.0121	
	5.1 Maximize employee integrity in the company	0.5	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.4	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.5	0.013	
	9.1 Create an environment that empowers employees	0.5	0.0155	
	9.3 Create an environment that promotes individual reliability	0.7	0.0155	
T54 - Open communication policy	2.1 Create an environment that promotes contribution	0.7	0.0149	**0.08414**
	2.2 Instill high levels of morale	0.5	0.0149	
	2.3 Increase/maintain pride in the organization	0.5	0.0149	
	2.4 Develop and maintain a motivated workforce	0.7	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.3	0.0121	
	5.1 Maximize employee integrity in the company	0.7	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013	
	9.1 Create an environment that empowers employees	0.5	0.0155	
	9.2 Create an environment that promotes respect	0.5	0.0155	

T55 - Contribution/matching program	2.1 Create an environment that promotes contribution	0.7	0.0149	**0.10171**
	2.2 Instill high levels of morale	0.7	0.0149	
	2.3 Increase/maintain pride in the organization	0.7	0.0149	
	2.4 Develop and maintain a motivated workforce	0.8	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0121	
	5.1 Maximize employee integrity in the company	0.5	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.013	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0195	
	9.3 Create an environment that promotes individual reliability	0.7	0.0155	
T56 - Teambuilding Exercises	2.1 Create an environment that promotes contribution	0.7	0.0149	**0.06461**
	2.4 Develop and maintain a motivated workforce	0.5	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0121	
	5.2 Create a desire to not jeopardize the reputation of the company	0.3	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.5	0.013	
	9.2 Create an environment that promotes respect	0.8	0.0155	
	2.2 Instill high levels of morale	0.5	0.0149	
	2.3 Increase/maintain pride in the organization	0.7	0.0149	

T57 - Provide training and development programs for career advancement	2.1 Create an environment that promotes contribution	0.5	0.0149	**0.10692**
	2.2 Instill high levels of morale	0.6	0.0149	
	2.3 Increase/maintain pride in the organization	0.6	0.0149	
	2.4 Develop and maintain a motivated workforce	0.8	0.0149	
	3.3 Create an environment that promotes organizational loyalty	0.7	0.0121	
	5.1 Maximize employee integrity in the company	0.8	0.0325	
	5.2 Create a desire to not jeopardize the reputation of the company	0.3	0.013	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.5	0.013	
	9.1 Create an environment that empowers employees	0.8	0.0155	
	9.3 Create an environment that promotes individual reliability	0.8	0.0155	
T58 – Ethics Hotline	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.9	0.0161	**0.01449**
T59 - Policy of no retaliation to employees who report suspected issues	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.7	0.0161	**0.01127**
T60 - Hiring policies (background and credit checks)	3.2 Instill professional-based work ethics	0.7	0.0265	**0.01152**
T61 - Chief Ethics Officer	9.4 Ensure adequate management oversight of organizational integrity issues	0.9	0.0128	**0.03727**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.8	0.0234	
T62 - Ethics Committee	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0128	**0.02896**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.8	0.0234	

T63 - Ethics officer reports to the board or audit committee	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0128	**0.02662**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.7	0.0234	
T64 - Periodic ethics questionnaires of employees	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0128	**0.02662**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.7	0.0234	
T65 - Employees reaffirm (written test) ethics policy on a periodic basis	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.7	0.0234	**0.01638**
T66 - Performance management including upward feedback	9.2 Create an environment that promotes respect	0.8	0.0155	**0.01240**
T67 - Performance evaluations	9.3 Create an environment that promotes individual reliability	0.8	0.0155	**0.0124**
T68 - Budget/Financial reviews	9.4 Ensure adequate management oversight of organizational integrity issues	0.7	0.0128	**0.00896**
T69 - Board and Audit Committee periodic review of business plans	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0128	**0.01024**

69 Value-driven Tasks by Rank

Table E.2: 69 Value-driven Tasks by Rank

Rank	Task	Impacts Sub-Objective
1	T1 – Security Awareness Training	4.1 Maintain personal accountability for system use
		4.2 Ensure appropriate levels of user access
		4.3 Ensure appropriate physical security
		4.4 Ensure user access is based on "need to know"
		4.5 Ensure adequate management oversight of access control
		5.4 Minimize temptation to use information for personal benefit
		6.1 Minimize inappropriate changes to data
		6.2 Ensure appropriate data integrity controls for the processing of data
		6.3 Ensure adequate management oversight of data integrity issues
		8.1 Emphasize importance of data privacy
		8.2 Ensure employee awareness against disclosure of sensitive data
		8.3 Ensure employees understand the repercussions of disclosing sensitive data
		8.4 Ensure that sensitive data is adequately secured
		8.5 Ensure adequate management oversight of privacy issues
2	T21- Amendments to Guiding Principles	1.1 Develop a management team that leads by example
		2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)
		3.2 Instill professional-based work ethics
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		5.4 Minimize temptation to use information for personal benefit
		8.1 Emphasize importance of data privacy
		8.2 Ensure employee awareness against disclosure of sensitive data
		8.3 Ensure employees understand the repercussions of disclosing sensitive data
		9.1 Create an environment that empowers employees
		9.2 Create an environment that promotes respect
		9.3 Create an environment that promotes individual reliability

3	T5 - Authorization procedures	5.4 Minimize temptation to use information for personal benefit
		6.1 Minimize inappropriate changes to data
		8.4 Ensure that sensitive data is adequately secured
		4.2 Ensure appropriate levels of user access
4	T4 - Pre-defined roles and rights	4.4 Ensure user access is based on "need to know"
		6.1 Minimize inappropriate changes to data
		4.2 Ensure appropriate levels of user access
		8.4 Ensure that sensitive data is adequately secured
5	T22 - Amendments to Code of Business Conduct and Ethics	1.1 Develop a management team that leads by example
		3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)
		3.2 Instill professional-based work ethics
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		5.4 Minimize temptation to use information for personal benefit
		8.1 Emphasize importance of data privacy
		8.2 Ensure employee awareness against disclosure of sensitive data
		8.3 Ensure employees understand the repercussions of disclosing sensitive data
		9.2 Create an environment that promotes respect
		9.3 Create an environment that promotes individual reliability
6	T51 - Compensation and incentives tied to performance	2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		5.4 Minimize temptation to use information for personal benefit
		9.1 Create an environment that empowers employees
		9.3 Create an environment that promotes individual reliability
7	T12 - Automated access monitoring system	4.4 Ensure user access is based on "need to know"
		6.1 Minimize inappropriate changes to data

8	T52 - Rewards program	2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		9.3 Create an environment that promotes individual reliability
9	T57 - Provide training and development programs for career advancement	2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		9.1 Create an environment that empowers employees
		9.3 Create an environment that promotes individual reliability
10	T55 - Contribution/matching program	2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		5.4 Minimize temptation to use information for personal benefit
		9.3 Create an environment that promotes individual reliability
11	T50 - Authority delegation (written document for empowerment)	2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		9.1 Create an environment that empowers employees
		9.2 Create an environment that promotes respect

12	T53 – Well-defined career paths	2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		9.1 Create an environment that empowers employees
		9.3 Create an environment that promotes individual reliability
13	T35 - Process design training	7.1 Understand the expected use of available information and its relation to individual business processes
		7.3 Ensure that appropriate organizational controls are in place
		7.2 Develop procedures for managing changes to business processes
14	T14 - Security administration group/policy makers	8.5 Ensure adequate management oversight of privacy issues
		4.5 Ensure adequate management oversight of access control
		6.3 Ensure adequate management oversight of data integrity issues
15	T54 - Open communication policy	2.1 Create an environment that promotes contribution
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.1 Maximize employee integrity in the company
		5.2 Create a desire to not jeopardize the reputation of the company
		9.1 Create an environment that empowers employees
		9.2 Create an environment that promotes respect
16	T10 - Well-defined job descriptions	4.4 Ensure user access is based on "need to know"
		6.1 Minimize inappropriate changes to data
17	T11 – Segregation of duties matrix	4.4 Ensure user access is based on "need to know"
		6.1 Minimize inappropriate changes to data
18	T17 - Edit and validation routines	6.2 Ensure appropriate data integrity controls for the processing of data
19	T56 - Teambuilding Exercises	2.1 Create an environment that promotes contribution
		2.4 Develop and maintain a motivated workforce
		3.3 Create an environment that promotes organizational loyalty
		5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		9.2 Create an environment that promotes respect
		2.2 Instill high levels of morale
		2.3 Increase/maintain pride in the organization

20	T18 – Reconciliation procedures	6.2 Ensure appropriate data integrity controls for the processing of data
21	T7 – Badges/key cards	4.3 Ensure appropriate physical security
		8.4 Ensure that sensitive data is adequately secured
22	T9 - Security guards	4.3 Ensure appropriate physical security
		8.4 Ensure that sensitive data is adequately secured
23	T45 – Nondisclosure agreement with repercussions	5.2 Create a desire to not jeopardize the reputation of the company
		5.3 Create an environment that promotes the organization's best interests rather than personal gain
		5.4 Minimize temptation to use information for personal benefit
		8.2 Ensure employee awareness against disclosure of sensitive data
		8.3 Ensure employees understand the repercussions of disclosing sensitive data
24	T2 - Limit the use of group accounts or generic IDs	4.1 Maintain personal accountability for system use
		4.2 Ensure appropriate levels of user access
		8.4 Ensure that sensitive data is adequately secured
25	T19 – Periodic error log audits	6.3 Ensure adequate management oversight of data integrity issues
26	T20 – Periodic review of reconciliations	6.3 Ensure adequate management oversight of data integrity issues
27	T6- Centralized system administration	4.2 Ensure appropriate levels of user access
		8.4 Ensure that sensitive data is adequately secured
28	T8 - Video surveillance	4.3 Ensure appropriate physical security
		8.4 Ensure that sensitive data is adequately secured
29	T3 - Password controls to force unique logons	4.1 Maintain personal accountability for system use
		8.4 Ensure that sensitive data is adequately secured
30	T61 - Chief Ethics Officer	9.4 Ensure adequate management oversight of organizational integrity issues
		3.4 Ensure adequate management oversight of developing and sustaining an ethical environment
31	T36 - Document and make known business processes	7.1 Understand the expected use of available information and its relation to individual business processes
32	T37 -Create and make known information classification standards	7.1 Understand the expected use of available information and its relation to individual business processes

33	T26 - IT Training and development	1.2 Ensure confidence/comfort level in using computers
		1.4 Ensure employees have adequate IT training
		1.5 Ensure IT capability level of staff
34	T62 - Ethics Committee	9.4 Ensure adequate management oversight of organizational integrity issues
		3.4 Ensure adequate management oversight of developing and sustaining an ethical environment
35	T43 - Amendments to Employee Manual	8.1 Emphasize importance of data privacy
		8.2 Ensure employee awareness against disclosure of sensitive data
		8.3 Ensure employees understand the repercussions of disclosing sensitive data
36	T63 - Ethics officer reports to the board or audit committee	9.4 Ensure adequate management oversight of organizational integrity issues
		3.4 Ensure adequate management oversight of developing and sustaining an ethical environment
37	T64 - Periodic ethics questionnaires of employees	9.4 Ensure adequate management oversight of organizational integrity issues
		3.4 Ensure adequate management oversight of developing and sustaining an ethical environment
38	T13 - Periodic review of user access roles and rights	4.5 Ensure adequate management oversight of access control
39	T33 - Individual development plans	1.4 Ensure employees have adequate IT training
		1.5 Ensure IT capability level of staff
40	T40 - Risk assessment activities	7.3 Ensure that appropriate organizational controls are in place
41	T41 - Periodic review of business process improvement program	7.3 Ensure that appropriate organizational controls are in place
42	T42 -Executive management oversight	7.3 Ensure that appropriate organizational controls are in place
43	T32 - Skills assessments and performance evaluations	1.4 Ensure employees have adequate IT training
		1.5 Ensure IT capability level of staff
44	T44 - Posters in the coffee room	8.2 Ensure employee awareness against disclosure of sensitive data
		8.3 Ensure employees understand the repercussions of disclosing sensitive data
		8.1 Emphasize importance of data privacy

45	T15 – Audit log reviews	4.5 Ensure adequate management oversight of access control
46	T16 - Review of termination lists (centralized review)	4.5 Ensure adequate management oversight of access control
47	T65 - Employees reaffirm (written test) ethics policy on a periodic basis	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment
48	T27 – Hire employees with adequate IT skills	1.2 Ensure confidence/comfort level in using computers
		1.5 Ensure IT capability level of staff
49	T58 – Ethics Hotline	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)
50	T66 - Performance management including upward feedback	9.2 Create an environment that promotes respect
51	T67 - Performance evaluations	9.3 Create an environment that promotes individual reliability
52	T60 - Hiring policies (background and credit checks)	3.2 Instill professional-based work ethics
53	T59 - Policy of no retaliation to employees who report suspected issues	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)
54	T34 - Budget for Training	1.4 Ensure employees have adequate IT training
55	T69 - Board and Audit Committee periodic review of business plans	9.4 Ensure adequate management oversight of organizational integrity issues
56	T38 - Create and manage a business process improvement program	7.2 Develop procedures for managing changes to business processes
57	T39 - Create and adhere to business process maturity/lifecycle model	7.2 Develop procedures for managing changes to business processes
58	T29 - Compensation programs aligned with company values	1.3 Create legitimate opportunities for financial gain

59	T68 - Budget/Financial reviews	9.4 Ensure adequate management oversight of organizational integrity issues
60	T31 - Goals and incentives tied to job descriptions and performance	1.3 Create legitimate opportunities for financial gain
61	T46 - Privacy officer	8.5 Ensure adequate management oversight of privacy issues
62	T47 - Incident response team	8.5 Ensure adequate management oversight of privacy issues
63	T49 - Oversee Privacy aspects of Security Awareness Training	8.5 Ensure adequate management oversight of privacy issues
64	T23 - Written in Job Descriptions	1.1 Develop a management team that leads by example
65	T24 - Compensation/incentive programs designed to influence management teams leading by example	1.1 Develop a management team that leads by example
66	T25 - Empowerment Training	1.1 Develop a management team that leads by example
67	T48 - Periodic review of public information	8.5 Ensure adequate management oversight of privacy issues
68	T28 - Standardized computer platforms	1.2 Ensure confidence/comfort level in using computers
69	T30 - Recognition programs	1.3 Create legitimate opportunities for financial gain

Calculations for Sensitivity Analysis

Table E.3: Sensitivity Analysis: Calculations for 100% Technical

100% Technical				
Task	**Impacts Sub-Objective**	**Score $v_i(x_i)$**	**Adjusted Global Weight (w_i)**	**Final Score**
T1 – Security Awareness Training	4.1 Maintain personal accountability for system use	0.7	0.0756	**0.6696**
	4.2 Ensure appropriate levels of user access	0.7	0.1034	
	4.3 Ensure appropriate physical security	0.5	0.1120	
	4.4 Ensure user access is based on "need to know"	0.7	0.1034	
	4.5 Ensure adequate management oversight of access control	0.7	0.0756	
	5.4 Minimize temptation to use information for personal benefit	0.7	0.0390	
	6.1 Minimize inappropriate changes to data	0.7	0.2062	
	6.2 Ensure appropriate data integrity controls for the processing of data	0.5	0.1766	
	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.1472	
T2 - Limit the use of group accounts or generic IDs	4.1 Maintain personal accountability for system use	0.5	0.0756	**0.0688**
	4.2 Ensure appropriate levels of user access	0.3	0.1034	
T3 - Password controls to force unique logons	4.1 Maintain personal accountability for system use	0.7	0.0756	**0.0529**
T4 - Pre-defined roles and rights	4.4 Ensure user access is based on "need to know"	0.5	0.1034	**0.2271**
	6.1 Minimize inappropriate changes to data	0.5	0.2062	
	4.2 Ensure appropriate levels of user access	0.7	0.1034	
T5 - Authorization procedures	6.1 Minimize inappropriate changes to data	0.7	0.2062	**0.2167**
	4.2 Ensure appropriate levels of user access	0.7	0.1034	
T6- Centralized system administration	4.2 Ensure appropriate levels of user access	0.5	0.1034	**0.0517**
T7 – Badges/key cards	4.3 Ensure appropriate physical security	0.7	0.1120	**0.0784**

T8 - Video surveillance	4.3 Ensure appropriate physical security	0.5	0.1120	**0.0560**
T9 - Security guards	4.3 Ensure appropriate physical security	0.7	0.1120	**0.0784**
T10 - Well-defined job descriptions	4.4 Ensure user access is based on "need to know"	0.5	0.1034	**0.1548**
	6.1 Minimize inappropriate changes to data	0.5	0.2062	
T11 – Segregation of duties matrix	4.4 Ensure user access is based on "need to know"	0.5	0.1034	**0.1548**
	6.1 Minimize inappropriate changes to data	0.5	0.2062	
T12 - Automated access monitoring system	4.4 Ensure user access is based on "need to know"	0.7	0.1034	**0.2167**
	6.1 Minimize inappropriate changes to data	0.7	0.2062	
T13 - Periodic review of user access roles and rights	4.5 Ensure adequate management oversight of access control	0.7	0.0756	**0.0529**
T14 - Security administration group/policy makers	4.5 Ensure adequate management oversight of access control	0.7	0.0756	**0.1560**
	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.1472	
T15 – Audit log reviews	4.5 Ensure adequate management oversight of access control	0.5	0.0756	**0.0378**
T16 - Review of termination lists (centralized review)	4.5 Ensure adequate management oversight of access control	0.5	0.0756	**0.0378**
T17 - Edit and validation routines	6.2 Ensure appropriate data integrity controls for the processing of data	0.8	0.1766	**0.1413**
T18 – Reconciliation procedures	6.2 Ensure appropriate data integrity controls for the processing of data	0.7	0.1766	**0.1236**
T19 – Periodic error log audits	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.1472	**0.1030**
T20 – Periodic review of reconciliations	6.3 Ensure adequate management oversight of data integrity issues	0.7	0.1472	**0.1030**

Table E.4: Sensitivity Analysis: Calculations for 100% Socio-Technical

100% Socio-technical				
Task	**Impacts Sub-Objective**	**Score $v_i(x_i)$**	**Adjusted Global Weight (w_i)**	**Final Score**
T1 – Security Awareness Training	8.1 Emphasize importance of data privacy	0.7	0.0578	**0.2270**
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0631	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0596	
	8.4 Ensure that sensitive data is adequately secured	0.5	0.1280	
	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0524	
T2 - Limit the use of group accounts or generic IDs	8.4 Ensure that sensitive data is adequately secured	0.7	0.1280	**0.0896**
T3 - Password controls to force unique logons	8.4 Ensure that sensitive data is adequately secured	0.7	0.1280	**0.0896**
T4 - Pre-defined roles and rights	8.4 Ensure that sensitive data is adequately secured	0.5	0.1280	**0.0640**
T5 - Authorization procedures	8.4 Ensure that sensitive data is adequately secured	0.7	0.1280	**0.0896**
T6- Centralized system administration	8.4 Ensure that sensitive data is adequately secured	0.8	0.1280	**0.1024**
T7 – Badges/key cards	8.4 Ensure that sensitive data is adequately secured	0.7	0.1280	**0.0896**
T8 - Video surveillance	8.4 Ensure that sensitive data is adequately secured	0.7	0.1280	**0.0896**
T9 - Security guards	8.4 Ensure that sensitive data is adequately secured	0.7	0.1280	**0.0896**
T14 - Security administration group/policy makers	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0524	**0.0367**
T21- Amendments to Guiding Principles	1.1 Develop a management team that leads by example	0.5	0.0418	**0.1111**
	8.1 Emphasize importance of data privacy	0.5	0.0578	
	8.2 Ensure employee awareness against disclosure of sensitive data	0.5	0.0631	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.5	0.0596	

T22 - Amendments to Code of Business Conduct and Ethics	1.1 Develop a management team that leads by example	0.7	0.0418	**0.1556**
	8.1 Emphasize importance of data privacy	0.7	0.0578	
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0631	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0596	
T23 - Written in Job Descriptions	1.1 Develop a management team that leads by example	0.7	0.0418	**0.0292**
T24 - Compensation/incentive programs designed to influence management teams leading by example	1.1 Develop a management team that leads by example	0.7	0.0418	**0.0292**
T25 -Empowerment Training	1.1 Develop a management team that leads by example	0.7	0.0418	**0.0292**
T26 - IT Training and development	1.2 Ensure confidence/comfort level in using computers	0.7	0.0418	**0.1431**
	1.4 Ensure employees have adequate IT training	0.7	0.0680	
	1.5 Ensure IT capability level of staff	0.7	0.0947	
T27 – Hire employees with adequate IT skills	1.2 Ensure confidence/comfort level in using computers	0.5	0.0418	**0.0682**
	1.5 Ensure IT capability level of staff	0.5	0.0947	
T28 - Standardized computer platforms	1.2 Ensure confidence/comfort level in using computers	0.5	0.0418	**0.0209**
T29 - Compensation programs aligned with company values	1.3 Create legitimate opportunities for financial gain	0.8	0.0524	**0.0420**
T30 - Recognition programs	1.3 Create legitimate opportunities for financial gain	0.3	0.0524	**0.0157**
T31 - Goals and incentives tied to job descriptions and performance	1.3 Create legitimate opportunities for financial gain	0.7	0.0524	**0.0367**
T32 - Skills assessments and performance evaluations	1.4 Ensure employees have adequate IT training	0.5	0.0680	**0.1097**
	1.5 Ensure IT capability level of staff	0.8	0.0947	
T33 - Individual development plans	1.4 Ensure employees have adequate IT training	0.7	0.0680	**0.1139**
	1.5 Ensure IT capability level of staff	0.7	0.0947	
T34 - Budget for Training	1.4 Ensure employees have adequate IT training	0.7	0.0680	**0.0476**

T35 - Process design training	7.1 Understand the expected use of available information and its relation to individual business processes	0.7	0.3271	**0.3845**
	7.3 Ensure that appropriate organizational controls are in place	0.7	0.1573	
	7.2 Develop procedures for managing changes to business processes	0.7	0.0649	
T36 - Document and make known business processes	7.1 Understand the expected use of available information and its relation to individual business processes	0.5	0.3271	**0.1636**
T37 -Create and make known information classification standards	7.1 Understand the expected use of available information and its relation to individual business processes	0.5	0.3271	**0.1636**
T38 - Create and manage a business process improvement program	7.2 Develop procedures for managing changes to business processes	0.7	0.0649	**0.0454**
T39 - Create and adhere to business process maturity/lifecycle model	7.2 Develop procedures for managing changes to business processes	0.7	0.0649	**0.0454**
T40 - Risk assessment activities	7.3 Ensure that appropriate organizational controls are in place	0.7	0.1573	**0.1101**
T41 - Periodic review of business process improvement program	7.3 Ensure that appropriate organizational controls are in place	0.7	0.1573	**0.1101**
T42 -Executive management oversight	7.3 Ensure that appropriate organizational controls are in place	0.7	0.1573	**0.1101**
T43 - Amendments to Employee Manual	8.1 Emphasize importance of data privacy	0.7	0.0578	**0.1263**
	8.2 Ensure employee awareness against disclosure of sensitive data	0.7	0.0631	
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.7	0.0596	
T44 - Posters in the coffee room	8.2 Ensure employee awareness against disclosure of sensitive data	0.5	0.0631	**0.0902**
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.5	0.0596	
	8.1 Emphasize importance of data privacy	0.5	0.0578	

T45 – Nondisclosure agreement with repercussions	8.2 Ensure employee awareness against disclosure of sensitive data	0.9	0.0631	**0.1104**
	8.3 Ensure employees understand the repercussions of disclosing sensitive data	0.9	0.0596	
T46 - Privacy officer	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0524	**0.0367**
T47 - Incident response team	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0524	**0.0367**
T48 - Periodic review of public information	8.5 Ensure adequate management oversight of privacy issues	0.5	0.0524	**0.0262**
T49 - Oversee Privacy aspects of Security Awareness Training	8.5 Ensure adequate management oversight of privacy issues	0.7	0.0524	**0.0367**

Table E.5: Sensitivity Analysis: Calculations for 100% Social

100% Social				
Task	**Impacts Sub-Objective**	**Score** $v_i(x_i)$	**Adjusted Global Weight** (w_i)	**Final Score** $\Sigma w_i * v_i(x_i)$
T21- Amendments to Guiding Principles	2.1 Create an environment that promotes contribution	0.5	0.0542	**0.4846**
	2.2 Instill high levels of morale	0.7	0.0542	
	2.3 Increase/maintain pride in the organization	0.7	0.0542	
	2.4 Develop and maintain a motivated workforce	0.5	0.0542	
	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.5	0.0585	
	3.2 Instill professional-based work ethics	0.7	0.0964	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0440	
	5.1 Maximize employee integrity in the company	0.5	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.0473	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0709	
	9.1 Create an environment that empowers employees	0.5	0.0564	
	9.2 Create an environment that promotes respect	0.7	0.0564	
	9.3 Create an environment that promotes individual reliability	0.3	0.0564	

T22 - Amendments to Code of Business Conduct and Ethics	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.6	0.0585	**0.2909**
	3.2 Instill professional-based work ethics	0.5	0.0964	
	5.1 Maximize employee integrity in the company	0.5	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.0473	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0709	
	9.2 Create an environment that promotes respect	0.7	0.0564	
	9.3 Create an environment that promotes individual reliability	0.3	0.0564	
T45 – Nondisclosure agreement with repercussions	5.2 Create a desire to not jeopardize the reputation of the company	0.7	0.0473	**0.1158**
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.0473	
	5.4 Minimize temptation to use information for personal benefit	0.7	0.0709	
T50 - Authority delegation (written document for empowerment)	2.1 Create an environment that promotes contribution	0.9	0.0542	**0.3575**
	2.2 Instill high levels of morale	0.9	0.0542	
	2.3 Increase/maintain pride in the organization	0.7	0.0542	
	2.4 Develop and maintain a motivated workforce	0.5	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0440	
	5.1 Maximize employee integrity in the company	0.5	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.0473	
	9.1 Create an environment that empowers employees	0.9	0.0564	
	9.2 Create an environment that promotes respect	0.7	0.0564	

T51 - Compensation and incentives tied to performance	2.1 Create an environment that promotes contribution	0.9	0.0542	**0.4125**
	2.2 Instill high levels of morale	0.8	0.0542	
	2.3 Increase/maintain pride in the organization	0.7	0.0542	
	2.4 Develop and maintain a motivated workforce	0.5	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.7	0.0440	
	5.1 Maximize employee integrity in the company	0.5	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.0473	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0709	
	9.1 Create an environment that empowers employees	0.7	0.0564	
	9.3 Create an environment that promotes individual reliability	0.6	0.0564	
T52 - Rewards program	2.1 Create an environment that promotes contribution	0.7	0.0542	**0.3919**
	2.2 Instill high levels of morale	0.8	0.0542	
	2.3 Increase/maintain pride in the organization	0.7	0.0542	
	2.4 Develop and maintain a motivated workforce	0.9	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.7	0.0440	
	5.1 Maximize employee integrity in the company	0.7	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.7	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.8	0.0473	
	9.3 Create an environment that promotes individual reliability	0.7	0.0564	

T53 – Well-defined career paths	2.1 Create an environment that promotes contribution	0.5	0.0542	**0.3179**
	2.2 Instill high levels of morale	0.7	0.0542	
	2.3 Increase/maintain pride in the organization	0.5	0.0542	
	2.4 Develop and maintain a motivated workforce	0.8	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.3	0.0440	
	5.1 Maximize employee integrity in the company	0.5	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.4	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.5	0.0473	
	9.1 Create an environment that empowers employees	0.5	0.0564	
	9.3 Create an environment that promotes individual reliability	0.7	0.0564	
T54 - Open communication policy	2.1 Create an environment that promotes contribution	0.7	0.0542	**0.3060**
	2.2 Instill high levels of morale	0.5	0.0542	
	2.3 Increase/maintain pride in the organization	0.5	0.0542	
	2.4 Develop and maintain a motivated workforce	0.7	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.3	0.0440	
	5.1 Maximize employee integrity in the company	0.7	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.0473	
	9.1 Create an environment that empowers employees	0.5	0.0564	
	9.2 Create an environment that promotes respect	0.5	0.0564	

T55 - Contribution/matching program	2.1 Create an environment that promotes contribution	0.7	0.0542	**0.3699**
	2.2 Instill high levels of morale	0.7	0.0542	
	2.3 Increase/maintain pride in the organization	0.7	0.0542	
	2.4 Develop and maintain a motivated workforce	0.8	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0440	
	5.1 Maximize employee integrity in the company	0.5	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.5	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.7	0.0473	
	5.4 Minimize temptation to use information for personal benefit	0.5	0.0709	
	9.3 Create an environment that promotes individual reliability	0.7	0.0564	
T56 - Teambuilding Exercises	2.1 Create an environment that promotes contribution	0.7	0.0542	**0.2349**
	2.4 Develop and maintain a motivated workforce	0.5	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.5	0.0440	
	5.2 Create a desire to not jeopardize the reputation of the company	0.3	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.5	0.0473	
	9.2 Create an environment that promotes respect	0.8	0.0564	
	2.2 Instill high levels of morale	0.5	0.0542	
	2.3 Increase/maintain pride in the organization	0.7	0.0542	

T57 - Provide training and development programs for career advancement	2.1 Create an environment that promotes contribution	0.5	0.0542	**0.3888**
	2.2 Instill high levels of morale	0.6	0.0542	
	2.3 Increase/maintain pride in the organization	0.6	0.0542	
	2.4 Develop and maintain a motivated workforce	0.8	0.0542	
	3.3 Create an environment that promotes organizational loyalty	0.7	0.0440	
	5.1 Maximize employee integrity in the company	0.8	0.1182	
	5.2 Create a desire to not jeopardize the reputation of the company	0.3	0.0473	
	5.3 Create an environment that promotes the organization's best interests rather than personal gain	0.5	0.0473	
	9.1 Create an environment that empowers employees	0.8	0.0564	
	9.3 Create an environment that promotes individual reliability	0.8	0.0564	
T58 – Ethics Hotline	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.9	0.0585	**0.0527**
T59 - Policy of no retaliation to employees who report suspected issues	3.1 Create an environment that makes it ok to report unethical behavior (whistle blowing)	0.7	0.0585	**0.0410**
T60 - Hiring policies (background and credit checks)	3.2 Instill professional-based work ethics	0.7	0.0964	**0.0419**
T61 - Chief Ethics Officer	9.4 Ensure adequate management oversight of organizational integrity issues	0.9	0.0465	**0.1355**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.8	0.0851	
T62 - Ethics Committee	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0465	**0.1053**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.8	0.0851	
T63 - Ethics officer reports to the board or audit committee	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0465	**0.0968**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.7	0.0851	

T64 - Periodic ethics questionnaires of employees	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0465	**0.0968**
	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.7	0.0851	
T65 - Employees reaffirm (written test) ethics policy on a periodic basis	3.4 Ensure adequate management oversight of developing and sustaining an ethical environment	0.7	0.0851	**0.0596**
T66 - Performance management including upward feedback	9.2 Create an environment that promotes respect	0.8	0.0564	**0.0451**
T67 - Performance evaluations	9.3 Create an environment that promotes individual reliability	0.8	0.0564	**0.0451**
T68 - Budget/Financial reviews	9.4 Ensure adequate management oversight of organizational integrity issues	0.7	0.0465	**0.0326**
T69 - Board and Audit Committee periodic review of business plans	9.4 Ensure adequate management oversight of organizational integrity issues	0.8	0.0465	**0.0372**

Vita

Jeffrey L. May was born on April 20, 1970 in Dayton, Ohio. He graduated from Trotwood Madison High School in Trotwood, Ohio in 1988. He received his BS in Mechanical Engineering from Wright State University in Dayton, Ohio in 1993 and graduated *Summa Cum Laude*. He then received his MS in Environmental Engineering from Virginia Tech in Blacksburg, Virginia in 1996 and an MS is Information Systems from Virginia Commonwealth University in Richmond, Virginia in 2003.

Jeffrey May is currently a faculty member at James Madison University in Harrisonburg, Virginia where he has been employed since 2007. Previously, he was a collateral faculty member and doctoral candidate in the Department of Information Systems at Virginia Commonwealth University in Richmond, Virginia. He had been teaching at VCU since 2000. Before 2000, he worked both as a pilot plant engineer and account manager.

Since 2000, he has taught over 50 classes, such as Computer Programming and Design, Introduction to IS, and Business Statistics and consistently has been evaluated as one of the top instructors at both VCU and JMU. His teaching interests include computer programming, systems analysis and design, database, and various other (IS) related topics along with decision analysis and statistics. His main goal in teaching is to provide his students with the ability to problem solve given various decision domains.

His research interests focus on organizational IS security. He believes that IS security consists of both technical and socio-organizational constructs and desires to create a program of research that will provide a consistent means for evaluating an organization's security in this context along with creating better IS security theories. Specifically, his future research will consist of developing multi-objective decision analysis models and auditing tools for evaluating and thus maximizing organizational IS security across various industry segments. Additionally, he is interested in applying decision analysis techniques to other IS-related topics and is also interested in Semiotics as it applies to problem solving.

His past publications include:

May, J. and Dhillon, G. (2007). "Investigating the Development of a Multi-objective Decision Model that Seeks to Generate Informed Alternatives for Maximizing IS Security within an Organization," AMCIS 2007, Keystone, Colorado.

May, J. and Dhillon, G. (2007). "An Analysis of the Fundamental Objectives of IS Security: Directions for Future Research," in *Proceedings of the 6th Annual Security Conference*, April 11-12, 2007, Las Vegas, NV.

Dhillon, G. and May, J. (2006). "Interpreting Security in Human-Computer Interactions: A Semiotic Analysis," in *Human-Computer Interactions and Management Information Systems Foundations*, Ping Zhang & Dennis Galletta (eds), M. E. Sharpe, Inc.

May, J. and Randall, C. (1996). "Investigating Bioremediation in Upflow Reactors Using Advanced Techniques (Biostyr)," WEFTEC '96: Proceedings of the 69th Annual Conference and Exposition of the Water Environment Federation, Dallas, TX, October 5-9, 1996.

May. J. and Hankey, W. (1993). "Investigating Aircraft Spin for the Stealth Bomber and F16," Presented at the First Annual Ohio Space Grant Consortium (OSGC), Ohio Aerospace Institute, Cleveland, OH, April, 1993. Voted as best undergraduate research in the field of Aerospace Engineering in Ohio for 1993.