2008

DEFINING VALUE BASED INFORMATION SECURITY GOVERNANCE OBJECTIVES

Sushma Mishra
Virginia Commonwealth University

DEFINING VALUE BASED INFORMATION SECURITY GOVERNANCE OBJECTIVES

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

by

SUSHMA MISHRA
Post Graduate Diploma in Business Administration (MBA equivalent)
International Management Institute, New Delhi, India, 1999

Bachelor of Science (Physics, Honors)
University of Calcutta, India, 1995

Director: Dr. Gurpreet Dhillon
PROFESSOR, INFORMATION SYSTEMS

Virginia Commonwealth University
Richmond, Virginia
May 2009

Acknowledgements

I begin with thanking my family for their patience in bearing with the rigorous demands of this profession. I most deeply want to thank my husband, Amit Pandey, for his unwavering faith and unconditional support to make this undertaking worthwhile. His unbounded enthusiasm, energy and passion have always inspired me to dream the impossible. Amit is my strength and a true companion in every sense. I also acknowledge my son, Arjuna Dev, whose birth gave me a fresh perspective towards life. I hope when he grows up and reads this, he would be proud of his mom. I appreciate the continued support from my mother-in-law and father-in-law during the writing of this dissertation and thanks to Anurag Pandey for always being there whenever I needed his help. I want to thank Dr. Satish Tripathi, a father figure in our lives, for his continued guidance and support and my brother, Sanjay for always believing in me.

This dissertation would not be possible without the intellectual support of my committee members. I extend my heartfelt thanks to Dr. Gurpreet Dhillon, my advisor, for working with me. I am still in awe of his immense dedication and vitality for research. The perfectionist that he is, he read every word of the multiple versions of this work and always came up with ideas to improve the work. Dr. Dhillon, I did learn a lot from you; as a scholar, as a teacher and as a friend. I thank all my committee members, Doctors Amita Chin, Roland Weistroffer, Richard Redmond and Anson seers for their support and encouragement. Thanks to Dr. Allen S. Lee, who has been a major influence in shaping my thinking as a scholar, about information systems.

I made several friends in the graduate school who not only provided unique insights into my scholarly activities but also extended constant encouragement and support. Thanks to Long Li, Gurvirendra Tejay, Dave Coss and Mark Harris for your friendship.

Also, I want to acknowledge my late dad, Shri Shew Dular Mishra, for helping me to be the woman that I am today. He will always be my hero! I dedicate this work to him.

Table of Contents

Page

List of Tables

Page

List of Figures

Page

Abstract

This research argues that the information security governance objectives should be grounded in the values of organizational members. Research literature in decision sciences suggest that individual values play an important role in developing decision objectives. Information security governance objectives, based on values of the stakeholders, are essential for a comprehensive security control program. The study uses Value Theory as a theoretical basis and value focused thinking as a methodology to develop 23 objectives for information security governance. A case study was conducted to reexamine and interpret the significance of the proposed objectives in an organizational context. The results suggest three emergent dimensions of information security governance for effective control structure in organizations: resource allocation, user involvement and process integrity. The synthesis of data suggests eight principles of information security governance which guides organizations in achieving a comprehensive security environment. We also present a means-end model of ISG which proposes the interrelationships of the developed objectives. Contributions are noted and future research directions suggested.

CHAPTER 1 Introduction

1.1 Introduction

This research is about designing internal control objectives for maximizing Information Security Governance (ISG) in organizations. Adequate internal controls are an essential part of the governance structure in an organization. The creation and implementation of these controls are essential in order to streamline organizational processes.

Security controls in the context of information security governance are primarily aimed at achieving three things: managing the business process integrity, ensuring business continuity and aligning organizational objectives with those of the security program (COSO, 2004). A poorly designed control structure is incapable of communicating top management's objectives and philosophy to the employees. Information security governance objectives convey the management's goals for the security program and its expectations from the organizational members for the achievement of these objectives. Lack of proper security governance objectives can lead to faulty design of controls, which result in information security problems. Hence, an understanding of the process of designing internal control objectives is imperative.

There is evidence in extant literature which points to a lack of understanding about the process of designing internal control objectives. Most of the prevalent internal control models are atheoretical and do not provide insight into the design process of such

objectives. This research also makes a contribution towards the design of internal control objectives for information security governance from a value-focused perspective.

The overall aim of this research is to develop information security governance objectives for organizations which are theoretically grounded and based on the values of the stakeholders. In pursuance of this aim, this study elicits individual values for internal controls in information security governance context, creates a means-end framework of fundamental objectives of internal control objectives, examines the theoretical framework through an in-depth case study and proposes ISG principles for implementation.

The remainder of this chapter is organized as follows. Section 1.2 presents the nature of the research and section 1.3 establishes the importance of the research problem. Section 1.4 presents the scope of the research and section 1.5 presents the structure and description of the whole dissertation.

1.2 Nature of the research

There is a surfeit of reported security breaches which have resulted in huge losses to organizations resulting from inadequate security controls. According to the Global Security Survey by Deloitte (2006), many financial institutions still have not felt the need to measure the effectiveness of their information security controls, leading to serious organizational vulnerability. Cases of serious insider breaches suggest two things:

First, the internal control objectives are incapable of checking and preventing such incidents proactively. Second, the control objectives are either inadequately conveyed to the organizational members or the objectives fail to motivate the members to align their personal objectives with security control objectives. The “tone at the top” is ineffective in

conveying the right message to the employees. When the individuals are unable to identify with the control objectives and the lack of alignment between individual and corporate goals is palpable, then this lacuna becomes evident through internal breaches.

This research argues that information security governance objectives of an organization should be grounded in the individual values of organizational members to provide a better control structure. Designing and implementing internal controls is an important part of effective information security programs. This study focuses on eliciting individual values for designing internal controls for information security governance. Studying the value propositions of employees for information security governance would identify the deep-seated values of people within organizations. This would facilitate a "bottoms up" approach for designing of control objectives and governance.

The basic research question that guides this research is "What are the information security governance objectives to be followed to keep organizations secure?" In pursuit of a comprehensive addressal of this question, the sub questions that need to be answered are:

1. What should be the nature and scope of ISG objectives for defining and developing internal controls such that information security can be maintained?
2. What are the principles to be adhered to in order to ensure good information security governance in an organization?
3. How can organizations improve their information security governance practices?

1.3 Importance of the research problem

Organizations face a major problem in the rampant lack of proper information security governance. Due to inadequate information security governance, security incidents are on the rise, making managers nervous about their ability to minimize risks and vulnerabilities in information systems. The concerns about security breaches in organizations are steadily increasing and can mainly be divided into four types (Parker, 2006):

- Increasing security incidents: The number of security threats is increasing, as evidenced by numerous surveys and research. According to CERT sources, security incidents have risen 2099 % from 1998- 2002- an average annual growth rate of 116 % (CERT, 2006).
- Sophisticated nature of security breaches: It is no longer a secret that most security breaches are caused by insiders. The new threats are becoming increasingly complex and sophisticated in nature. Currently rampaging viruses have the capability of shutting down the entire IT network in the organization.
- Increasing regulatory pressure: Many governmental regulations have acknowledged the importance of information security in the knowledge economy. Regulations such as the Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act (GLB) and the Health Insurance Portability and Accountability Act (HIPAA) provide a lot of institutional pressure for better security preparedness. There are strict requirements in the form of internal control management processes, which are pushing up the strategic importance of security in organizations.

- Dynamic security needs: Reactive and ad hoc security measures can only provide temporary relief from particular kinds of security threats. Security management has to be proactive to enable flexibility on the part of management to combat unseen threats. This needs to be inbuilt in the system and adaptive modular approaches need to be installed.

So how do organizations deal with the situation? Global security surveys conducted by four major consulting firms (Deloitte, KPMG, PWC and E&Y, 2006) to understand organizational responses to security problems show: more awareness of security as a strategic issue in organizations, more investments in security programs, increased acceptance of the reality of internal threats and more security issues in boardrooms, as compared to any other year. Even though there is an increase in security awareness of organizations, the numbers of security attacks and resulting breaches have recorded a corresponding rise to reach an unprecedented level. It is an indicator of the fact that organizations are unable to generate fundamental and effective responses to security issues in general.

The lack of effective information security governance in organizations is a result of security governance objectives being inadequately defined and implemented. If the objectives are not in place, it naturally follows that there cannot be adequate controls to achieve them. This is made evident by the fact that most security breaches are not technical but socio-organizational in nature. A study on security breaches in finance industry reported that most security incidents were not technically sophisticated. These incidents typically involved exploitation of vulnerabilities such as business rules or organizational

policies (CERT 2004). The lack of proper information security governance objectives in organizations are manifested in two ways: inadequate internal control structure and increased insider threats. Most of the recent security failures can be traced to either of these two consequences of inadequate ISG.

There is a plethora of reported security breaches resulting in huge losses to organizations, which are a direct result of inadequate controls. The recent 2008 episode at Societe Generale where more than 4 billion Euro were wiped out of the banks assets by an insider is a pertinent example. The organization has blamed employee Jerome Kerviel for the colossal loss. He has been charged with hacking into the bank's computers, falsifying documents and breach of trust (Forte and Power, 2008). Kerviel circumvented obsolete procedures about reporting transactions in the bank and exposed it to exceptionally high risks in the futures trading market. The banks losses were in the region of $7 billion and it is speculated that this breakdown fueled the U.S. Federal Reserve's emergency 0.75% rate cut in interests. The bank also confirmed that it has instituted "additional control procedures" to prevent a reoccurrence of similar rogue trading in the future (Forte and Power, 2008).

Some of the most glaring examples of security failures of catastrophic proportions can be attributed to inadequate control structures in organizations. Fiascos such as the demise of the Barings Bank, Kidder Peabody and the above mentioned Societe Generale case reflect on the inability to institute adequate internal controls and Enron's failure to ensure integrity of business processes clearly point to the increasing need for effective control structures.

Cases of lack of integrity leading to lapses in information security governance abound. Recently the office of Ohio Secretary of State posted SSNs, date of births and personal information of citizens on a state website as part of Standard Security Practices (Privacy Rights Clearinghouse 2006). The Department of Social Services in Los Angeles reported boxes of files containing personal identifiable information such as W-2, medical information and SSN being left unattended and unshredded, which exposed more than 2,000,000 individuals to security risks (Rutgers Identity Theft Center, 2006). These breaches are a glaring example of the lack of adequate internal controls and poor implementation of controls that do exist. It is not surprising that the argument to "make information security a boardroom issue" (Coviello and Swindle 2006) is being repeated and is gaining validity. Cyber Security Industry Alliance, in its National Agenda for Information Security for 2006 has urged the Federal Government to encourage private sector to apply information security governance to business operations (p.6). There is clearly a gap between management's objectives for information security governance and employees' understanding of the same. There remains a palpable lack of proper written security policies in organizations, especially in industries which are not extensively IT dependent such as financial sector, education and government (Leyden, 2004). Many well known episodes of business infidelity are an example of the vulnerability of state of the art information security governance to break-ins and exploitation of the existing vulnerabilities in the business process (Forte and Power, 2008).

Information security governance encompasses various aspects of organizational functions. The design and development of applications to support the infrastructure for business

process and mechanisms for deploying these applications are under the purview of security management. Also, policy development and implementation, internal control design and implementation, management of technology and people; all of these constitute part and parcel of the information security governance in an organization.

Another indicator of the lack of adequate ISG objectives, which is the internal threat from employees, has always been acknowledged as a major source of security breaches in organizations. 96% of the respondents in global security survey conducted by Deloitte indicate that they are concerned about employee misconduct involving their information systems (Deloitte, 2006). The survey identifies the majority of threats as being due to errors and omissions (human error: 42%; operational error: 37%), rather than malicious intent. It is important to note that, of those institutions that experienced a successful internal breach, 28% were the result of experienced and intentional fraud and 18% were due to the intentional leaking of customer data (Deloitte, 2006).

The numerous cases of serious insider breaches suggest two things as already mentioned: First, the ISG objectives are incapable of checking and preventing such incidents proactively. Second, the control objectives are either inadequately conveyed to the organizational members or are not aligned with their personal objectives in an effective way. The "powers that be" are ineffective in conveying the right message to the employees, resulting in the employee's isolation and alienation from the control objectives. The apparent lack of alignment between individual and corporate goals is manifested in internal breaches.

This leads to a significant question: What are the businesses doing about this situation?

It is not clear how organizations plan to combat these issues in security governance. The global security survey conducted by Price Waterhouse Coppers (PWC) shows that most executives with security responsibilities in organizations worldwide have made little progress in implementing strategic security measures that could have acted as a fundamental inhibitor for various security incidents (PWC, 2006). Since, security governance objectives are not being developed at the corporate level and are not being integrated in the business processes, the risks in form of increased insider threats and failure of controls still remain. Also, the lack of planning in governance objectives obviously results in more reactive than proactive measures for dealing with security threats.

Security is still perceived as a cost driver and not a value creator. Majority of the organizations reported that their security is not in compliance with major regulations, such as Health Insurance Portability and Accountability Act (HIPPA), Sarbanes Oxley Act or non-U.S laws such as European Union Data Privacy Directive, which have been around for years (PWC, 2006). Thus mandating internal control assessment through regulations is obviously not serving the purpose.

Information security governance practices depend on strong internal control management techniques and a supportive control environment in an organization. Organizations that reported their security polices and spending are more aligned with their business processes experienced fewer financial losses and less network downtime than those that did not (PWC, 2006). This is an indicator of the dire need for effective information security governance programs in organizations. Correct information security governance objectives

are required to assure proactive and encompassing security measures which protect organizations from threats. It is crucial to develop the right controls objectives and the requisite controls to compliment these objectives along with their periodic assessment. The overall security status of the organization is determined through an adequate assessment of the controls (NIST special publication 800-53A, 2006). The selection and implementation of security controls have major implications on the operations and assets of an organization. Security controls are the safeguards that maintain the integrity of the organizational information systems. The effectiveness of security controls must be assessed to determine the extent to which the controls are implemented correctly, their operation as per intention and requirement, and their effectiveness in producing the desired outcome with respect to meeting the security requirements for the system (NIST special publication 800-53A, 2006).

1.4 Scope of the research

Three categories of definitions are required for anchoring the basic concepts in this research. This section explicitly defines what we mean by information security, internal controls, information security governance and individual values in this research. A cogent definition of the basic constructs that guide this research will help the reader gauge the conceptual foundation of this work.

Information security: Information security means protecting all information assets from misuse, harm or any other unintended result. This includes securing information in computers, maintaining integrity of business processes, retaining skilled knowledge workers with their implicit knowledge and also encouraging employees to claim ownership

of their share of information assets (Dhillon 2006). Information is a shared asset, which has to be protected from all possible distortions by everyone sharing it. This definition adopts a holistic view of information systems security where information is secured through technical, organizational and normative means.

Internal controls: Internal controls are a means to provide reasonable assurance that an organization will achieve its business objectives while avoiding undesired risks (ISACA, 2004). Internal controls are policies, procedures, practices, and organizational structures put in place to reduce risks. These also attempt to rationalize the organizational processes. They operate at all levels in an organization and help in reducing risks involved at various stages of the operation, thus helping the organization reach its business objectives (Dhillon and Mishra, 2006).

Information security governance: ISG can be defined as "a way of establishing and maintaining a control environment to manage risks that relate to confidentiality, integrity and availability of information and its supporting processes and systems (Moultan and Cole, 2003)". This conceptualization suggests a technical orientation for security. Certified Information Systems Auditor (CISA) Review Manual (2004) defines information security governance as a "focused activity with specific value drivers: integrity of information, continuity of services and protection of information assets (pp.385)". This definition suggests that due to global integration of organizations via networks, security has become a significant governance issue and the end product of information security governance process is the safety and security of data.

Values: Value refers to the preferred or what is conceived as preferable to human mind (Catton, 1954). An individual's preferential behavior shows certain regularities and this pattern can be attributed to some standard or code, which persists through time providing a basis by which people order their intensities of desiring various desiderata (something desirable). Keeney (1992) conceptualizes value as "what we care about and should be the driving force for our decision making (pp. 3)". Values are more fundamental to a decision context than the available alternatives. But in common practice, decision-making usually focuses on the choice among existing alternatives.

Information systems security research has witnessed limited theory-developing efforts (Weber, 2006). Specifically in the area of internal controls design and implementation for security, there have been limited attempts to create or use existing theories. In this research, a theory building exercise is performed. By analyzing individual values about internal controls in organizations, we create a framework of means and fundamental objectives. The conceptual framework thus developed provides a set of high-level principles for internal controls design and implementation in the context of information security. The interrelations between various objectives also provide an insight into complex relationships and multipurpose roles that such objectives play.

This study is conducted using value theory as the theoretical basis and value focused assessment as a methodology. Catton (1954) proposed value theory, which states that the choices made by individuals over a period of time, shows a definite pattern and is guided by the values internal to such people. The values, deep rooted in people's minds, are manifested by the choices people make in complex situations. This theory provides an

appropriate basis for understanding the reasons for behavior of individuals in groups. Keeney (1992) suggests a methodology to create decision objectives by studying individual values in a decision context. This methodology- namely value focused thinking, provides a way to elicit individual values and creates decision objectives about a problem. A means-end framework can be created through this methodology, which provides high-level guidance in decision-making.

The framework developed is used to explain ISG conceptualizations and practices through an in-depth case study. This case study was conducted in the information technology department of a state agency in Virginia, USA. The results from the interviews and secondary data from the organization were used to reexamine the preliminary theoretical model.

1.5 Dissertation Structure

Chapter two presents a review of the extant research literature. In this research, we have primarily looked at three streams of research: information security research, management controls or organizational design research literature and internal controls research in information systems discipline.

Chapter three describes the theoretical basis and research methodology that this particular research adopts. A discussion about value theory as a theoretical basis and value focused thinking as a methodology is provided to conceptually ground the work.

Chapter four describes the creation of a means-end framework through the process of interviewing information security professionals across industries. Using Keeney's value

focused approach, a theoretical framework with means and fundamental objectives about internal controls for information systems security is created from the interview data.

Chapter five describes a case study that was conducted to create an initial conceptual framework about means and fundamental objectives regarding internal controls. In this theory building exercise, this chapter also presents a validation of the theoretical model.

Chapter six describes data analysis results and their implications for information security governance research in particular and information security research in general. The synthesis of the results is presented and an answer to the "so what" question of this research is provided.

Chapter seven presents a mapping of our initial research questions to our findings. The research contributions and limitations are suggested. Future research directions stemming from this work are also suggested.

CHAPTER 2 Literature Review

2.1 Introduction

The focus of this research is to develop internal control objectives for information security governance. There is little research in the area of information security governance (McFadzean et al., 2006; von Solms, 2006) and the available models have different conceptualizations about the topic. For this research, as described in the previous chapter, Information security governance is defining, implementing and monitoring security controls (ITGI, 2004). Since it is a subset of information systems security research, it is natural that research perspectives and trends in information systems security would influence this research. Therefore, to gain an insight into the research in information systems security governance, it is important to understand the prevalent research issues in information systems security domain. Information systems security places more emphasis on technical aspects of security than on its non-technical aspects in an organization (Baskerville, 1993; Dhillon, 2001; Backhouse and Dhillon, 2001). Information systems security research has traditionally been mechanistic in approach with a narrow focus on ensuring confidentiality, integrity and availability of the data in the computer systems (Dhillon and Torkzadeh, 2006; Baskerville and Sipponen, 2002). The narrow technical approach overlooks other major organizational security vulnerabilities to information systems in the form of lack of segregation of roles, disgruntled employees and inadequate security policies (Dhillon and Torkzadeh, 2006). Thus, it is not surprising that a review of information systems security governance research shows similar trends and biases to be inherited from the superset i.e. information security.

Two broad orientations dominate the literature in information systems security governance area: These are technical and socio-organizational orientation. Technically oriented security governance research places a greater emphasis on using technical controls (such as access controls and security architecture) to manage enterprise security. Socio-organizationally oriented security governance literature revolves more around formal and informal controls (such as responsibility and accountability and control culture) to ensure comprehensive security programs. A critical review of information systems security governance models from research and industry standards for governance is presented. The two perspectives described above are used to traverse the extant literature in information systems security governance.

The remainder of this chapter is divided into four sections. Following the introduction, the first section discusses the technically oriented information systems security governance literature. The second section discusses socio-organizationally oriented information systems security governance literature. The third section discusses the current state of extant literature in information systems security governance and analyzes its implications. This discussion also presents the gaps in the literature as identified in the review. Finally, the concluding section presents the assertions as these related to ISG practices.

2.2 Information Systems Security Governance: A Technical Orientation

As conceptualized by Moulton and Coles (2003), information systems security governance from a technical perspective can be defined as "a way of establishing and maintaining a control environment to manage risks that relate to confidentiality, integrity and availability of information and its supporting processes and systems." Along similar

lines, Certified Information Systems Auditor (CISA) Review Manual (2004) defines information security governance as a "focused activity with specific value drivers: integrity of information, continuity of services and protection of information assets (pp.385)". This definition suggests that due to global integration of organizations via networks, security has emerged as a significant governance issue and the end product of information security governance process is the surety of safe and secure data.

As mentioned above, research from this perspective is premised on the belief that security governance is about managing the confidentiality, integrity and availability of data in information systems. The emphasis is greater on data management than systems management. With a technical scope, control objectives developed and controls deployed focus on securing critical information in computer systems. The motivation being that technical safeguards are the most important component of a security program and if technical controls are in place, the organization is automatically more secure. Not only some research models but also some of the prevalent security governance standards have had technical focus.

ISO 17799, renamed as ISO/IEC 27002, is a prominent information security governance framework with a technical orientation to security management. International Standards Organization joined hands with International Electrotechnical Commission (IEC) for developing a series of standards for Information Security Management (ISM). These standards are the best practices for security management and are also known as ISO/IEC 27000 (ISO27K) series of standards. As per the new release on security management, ISO27k "provides the means to implement effective information security management in

compliance with organizational objectives and business requirements". Although preliminarily released in 2006, ISO27k is far from complete. Currently only three standards have been officially published (27001, 27002, and 27006) covering implementation and maintenance of an ISM system, guidelines for conducting ISM in an organization, and guidance for bodies that provide audit and certification of ISM systems. There is a future expectation about many more such security standards.

ISO/IEC 27002 is a widely used information security management framework in North America and Europe. The framework provides guidance about security in 11 different areas (see table 2.1). ISO/IEC 27002 is exclusive to information security, and only addresses that issue. It is divided into 10 sections, with 36 objectives. Each objective is again divided into sub-objectives (ISO, 2005)

The framework provides the range of controls needed for securing information systems. It is based on security risks assessment and provides the basis for cost justification and improved productivity of security staff.

The major benefit of using ISO/IEC 27002 for information security governance is that it is detailed and is targeted at people responsible for technical information security. The framework provides much more guidance on precisely 'how' things must be done (von Solms, 2005). For example it gives guidance on what an information security policy should look like in terms of structure and content. ISO/IEC 27002 is, in many cases, the framework of choice of IT and information security managers because of its technical superiority (von Solms, 2005).

Table 2.1. Control Objectives from ISO/ IEC 27002

Control objectives from ISO 17799	
1.	Business continuity planning
2.	Systems access control
3.	System development and maintenance
4.	Physical and environmental security
5.	Compliance
6.	Personnel security
7.	Security organization
8.	Computer and Network management
9.	Asset classification and control
10.	Security policy
11.	Incident management

There are some shortcomings of using this framework. It provides 'stand alone' guidance with a narrow focus on security management and cannot be integrated easily into a wider framework for information technology governance (von Solms, 2005; Brown and Nasuti, 2005). The framework does have a list of proposed controls but fails to suggest how these controls can be synchronized to achieve the maximum benefit (Eloff and Eloff, 2005). A marked emphasis on just the technical aspects of security management makes it incomplete as a framework for security governance area. With similar orientation, Information Technology Infrastructure Library (ITIL) is a widely used framework for referencing security management principles. The framework was developed in UK by the Office of Commerce. It identifies a broad range of processes that are considered as best practices for information technology service management (see table 2.2).

ITIL provides security from the service provider perspective, identifying the relationship between security management and IT security officer (ITIL, 2007). It describes the role of best practices for IT services. There are several guidelines in ITIL libraries about the technical management of security. Targeted at people responsible for IT service management, ITIL is a collection of books referred as best practices for IT service management (Heschl, 2004).

The key to the growing success of ITIL is its flexibility. ITIL, unlike other process-focused strategies for business improvement is not a methodology *per se*. ITIL consists of several libraries of advice and guidance on how to deliver and support IT services. However, there are many challenges which emerge while implementing ITIL in organizations. Implementing ITIL brings about sweeping changes in an organization in the form of changed processes and culture (Lange, 2007). It is difficult to assess the "value" that is added by implementing these changes. Also, ITIL is perceived as difficult to implement considering the huge volume of advice that it offers. The framework currently offers a library of 10 books on various IT service management topics. Organizations find it hard to fully comprehend the meaning of the framework (Lange, 2007). In summary, ITIL is high level, nonspecific and concentrates mainly on service of IT.

Table 2.2. Service processes as identified by ITIL

Service processes from ITIL
1. Incident management
2. Change management
3. Problem management
4. Configuration management
5. Release management
6. Service level management
7. Continuity management
8. Capacity management
9. Financial management
10. Availability management
11. Security management
12. Help desk management

Managing security risks from the Internet is a challenge from the information systems security governance perspective. Occurrence of business risks is becoming more imminent as the corporate network, processes and critical business data are vulnerable to attacks from the Internet (Segev et al., 1998). Denial of service attack is one of the big threats to organizational security. Abouzakhar and Manson (2002) suggest innovative ways to address different types of distributed denial of service attacks which have the ability to respond quickly. The authors acknowledge the attacks on networks as a significant security breach and in their suggestions to deal with these attacks they propose a model, with intelligent fuzzy agents, which allocate resources dynamically to ensure availability of the network for legitimate users without blocking useful protocols. This model is useful for

managing security from specialized external threats, although it does not provide any inputs for managing network breakdown threats from inside the organization.

Acknowledging the importance of managing Internet security threats, Qiang and Hua-ying (2007) argue that Internet security governance is an iterative and continuously evolving process. The authors propose a systematic model for the Internet security governance based on the complexity theory and systems dynamics. The authors analyze the topology characters of host objects and message spreading rules in the model. According to the model, Internet security governance has four stages; Nodes identification (identify the nodes which can carry viruses or messages that disrupt the system), topology structure analysis (typology affects the spreading trends of the diseases or viruses depending on the content on the web page), disease spreading analysis (describes the spreading speed of the disease, its coverage, duration and so on) and security governance (suggests measures to control the spreading of the disease in the network and verifies the measures through systems simulations and case studies). The above model treats the Internet as a technical system and does not acknowledge the importance of social and behavioral factors in managing risks. The model forwards too simplistic a representation of the real threats to the organizational networks on the Internet.

Along similar lines, with emphasis on technical supremacy to deal with information security problems, Finne (1996) proposes an information security chain model for security management in an organization. The model comprises twelve modules and eighty sub modules, each emphasizing an area of security management. The model has a heavy technical emphasis with modules such as computer security, distributed systems, operation

security, protection against theft, protection against fire and water, electricity distribution, internal and external threats, communication, external contact, contingency planning, personnel security, contract employees and visitors, attitude towards security issues, security questions and the environment. The model is comprehensive and touches upon the various sources and aspects of a security breach. But a model of this nature is too broad in scope and does not take into account the contextual security governance challenges that an organization faces.

In technically oriented security governance research, information security architecture is considered a crucial aspect of governance. From this perspective, researchers use security objectives as overarching access control and authentication rules for a computer system (e.g. Sandhu & Samarati, 1994). Sherwood (1996) argues that enterprise security architecture is extremely important to adequately comprehend and manage the security needs of the organization. Sherwood (1996) proposes a security governance model namely Sherwood Associates Limited Security Architecture (SALSA). In this multi-layered model, the top layer is the business requirements definition stage and at each subsequent lower layer, a new level of abstraction is developed. The lower layers define major security strategies, security services and security mechanisms. The last layer suggests ways of selecting technologies and products. This process approach to security management encourages everyone to participate in the security development program. The model helps in developing a participative security architecture which provides technical capabilities to meet the business requirements. For this reason, the model is more anecdotal and conceptual in nature rather than being driven by a theory or rigorous research. The

inconsistent implementation of security management controls is considered a major risk in today's networked environments. This is a significant security issue as there is no benefit in installing sophisticated access controls on one system to create a "trusted environment" when those controls can be simply bypassed by an unauthorized user gaining access to that "trusted environment" through a gateway connected system which has inadequate controls installed (Ward and Smith, 2002). Lack of proper controls results in exposing organizations to new vulnerabilities and compromising the confidentiality, integrity and availability of information systems. Development of access control policies to protect all systems is essential while implementing effective internal control processes consistently across all systems (Stoupa and Vakali, 2007).

Ward and Smith (2002) articulate the need for access control policies for information systems. The authors argue that is important to have governance guidelines and risk management strategies to protect information assets of an organization. Access control policies help the management in mitigating risks within the organization and allow effective segregation of roles for overall enterprise security. The paper proposes a high level approach to implementing security governance objectives through information security responsibilities, management accountability policy, and other access control security policies in individual and distributed systems. The proposed model adequately emphasizes the importance of access controls for networked environment. The model is limited in its application at an enterprise level as there is asymmetrical emphasis on access control policies compared to other technical requirements for governance. The proposed

model has not been tested in real organizational setting, thus its applicability is questionable.

Booker (2006) emphasizes the importance of maintaining a database of critical network and information assets for effective information systems security governance. It is a challenge to proactively manage security programs and minimize costs of the security initiatives. To overcome the above problem, a security management model is suggested. The model consists of five components (see table 2.3):

Table 2.3: Security management model (Booker, 2006)

Stages	Objectives
1.	Understanding disruptive forces
2.	Implementing a holistic approach
3.	Measuring and communicating value
4.	Aligning key security initiatives with business strategy
5.	Managing the program globally while allowing regional control

In *understanding disruptive forces* component, the author emphasizes the importance of governance and compliance, mobile workforce, business justification requirement and reactivity of businesses and suggests measures to deal with these issues. *Implementing a holistic approach* suggests that it is important to map security requirements into a simple taxonomy that provides a comprehensive security framework. For *measuring and communicating value*, it is suggested that calculation of Total Economic Impact (TEI) is used as it provides a better foundation for communicating the investment profile required for information security. Under *aligning key security initiatives with business strategy*, the author suggests that network security, communications security, identity management and operational risk management are necessary. And finally under *managing the program*

globally while allowing regional control component, alignment of global practices based on proven and acknowledged security standards, such as ISO17799, is recommended. This helps the business to document its security practices both internally and to the customers and trading partners. The model suggests that professional security operations must deliver security for the IT environment with appropriate value, service levels and accountability to the top management of the enterprise. This model is technically oriented and undermines the importance of social and behavioral influences on security management. The proposed model is generalized and lacks focus on "how" to operationalize the above ideas.

The research in information systems security governance area with a technical focus can be summarized as follows:

Security governance is viewed as managing confidentiality, integrity and availability of data. Hence emphasis on technological infrastructure is more in order to prevent the presence of technical loop holes in the systems.

1. Information systems security governance models are primarily focused on information systems security architecture, authentication, access control, Internet security and network management.
2. Security control objectives are derived from the technical requirements of the organization. It is assumed that if security is managed on the technical front, it would automatically make the overall organization secure.
3. Strong technical solutions to ensure security are adequately understood, implemented and used by the end users as intended by the management.

4. It is believed that for a governance model to be successful, organizations require coordinated incident response as well as a comprehensive knowledge framework of network, applications and business requirements.

Use of such technically oriented models is more popular as businesses are eager to grasp the idea of implementing complex technological controls to protect the information held in their computer systems (Dhillon, 2006). The governance models reviewed in this section encourage competent technical capabilities to support the entire security portfolio.

2.3 Information Systems Security Governance: A Socio-Organizational Orientation

Socio-organizationally grounded research in information systems security governance is premised upon the belief that management of formal and informal environment in an organization is more important than the management of the technical requirements. The research in this area emphasizes the importance of formalized procedures and individual inputs in the governance process. Researchers in this domain highlight the management's role in security governance. The management requires control objectives to define the goal of implementing policies, procedures, organizational structures and responsibilities to ensure that business objectives are met and undesirable events prevented. There are several existing frameworks for information systems security governance, in research and in practice, that advocate the socio-organizational approach to security management.

Grounded in socio-organizational perspective, Control Objectives for Information and Related Technology (CobiT) provides guidance on management's role in security management. It is the most widely used information technology (IT) governance standard

in United States. The framework provides “good practices” across a domain and a process framework that presents activities in a manageable and logical structure (ITGI, 2007). CobiT helps an organization align its business goals with IT goals. It emphasizes the importance of business needs that are satisfied by each of its objectives (Ridley et al, 2004).

CobiT provides seven criteria that generally define what business requires of IT (see figure 2.1). CobiT requires IT to deliver the information that an organization needs to meet its objectives. The framework divides IT processes into 34 types and categorizes these into four domains: Plan and Organize, Acquire and Implement, Delivery and Support, and Monitor and Evaluate. These domains contain 34 high level control objectives and 215 sub control objectives. These objectives are implemented through the use of control practices.

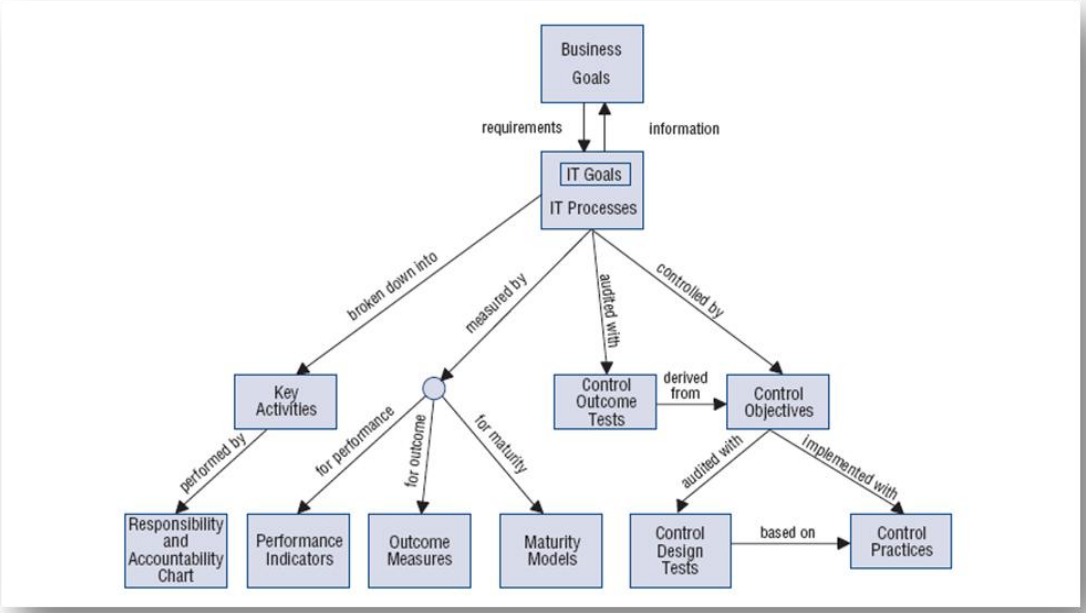

Figure 2.1. Interrelationships of COBIT components (source: COBIT 4.1, ITGI 2007, pp. 8)

CobiT is continuously kept up to date and harmonized with other standards and guidelines. There are several benefits of using CobiT as a governance framework for IT. Some of these are: better alignment with business, a simplistic view of IT's role in the organization, process orientation allowing ownership and responsibilities and CobiT popularity with third parties and regulators. CobiT is designed to provide more focus on aligning IT control objectives with the business processes of an organization and allows management to benchmark its control environment to standards of policy and good practices implemented worldwide (Ward and Smith, 2002).

Use of CobiT for information systems governance is not without criticisms. The framework represents the consensus of experts on good practices but it is not theory driven or empirically validated in research. The model is strongly focused on control and less on execution. The control objectives are very high level and generic and are not specifically tailored for security purposes. There is only one control objective that talks about security in any detail. DS5 is a high level control objective which says "Ensure System Security" and has 21 sub objectives to it. But these are not the only objectives relevant for information security governance (von Solms, 2005).

Along similar lines, Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework also describes a unified approach for evaluation of the internal control system that a management designs with the objective of achieving reasonable assurance of the fundamental business objectives. COSO was developed to provide consistent platform for developing and measuring effective internal controls across industries. The COSO framework suggests five control components (see table 2.4). These are:

Table 2.4. COSO components

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

The control environment defines the tone of an organization and the way it operates, providing both discipline and structure. Organizations with effective control environments set a positive example from "top management" and try to create integrity and control consciousness. This objective primarily provides the ethics, direction and philosophy to the organization (Dhillon and Mishra, 2006). Ramos (2004) argues that control environment is the foundation for all other components of internal controls. The risk assessment component suggests a process through which the management identifies the potential threats that can prevent the organization from meeting its business objectives. The controls activities include the operationalization of policies and procedures that are created and established to show management's intention of securing its assets. There could be several controls such as access control, physical controls, verifications and segregation of duties. The nature of the activities creates awareness and responsibility among the people who undertake the tasks. The information and communication component

emphasizes on reports containing operational information. Organizations need tools to capture and communicate relevant information to ensure the integrity of controls. Information thus obtained is critical to the processes of conducting, managing and controlling the operations of the organization. The monitoring component ensures that systems that are performing as intended controls are delivering the desired results. Monitoring can be accomplished by continuous checks and balances that occur during normal operations or also through separate evaluations by management, with the assistance of the internal auditors. The extent of ongoing monitoring usually determines the need for separate evaluations. The latest version of the COSO consists of eight components as three more controls have been added to the existing five controls. These are: objective setting, event identification and risk response.

The popular model COSO is not without its criticism. The set of objectives suggested in this model are all from the management perspective and the importance of maintaining a technical infrastructure is not emphasized. Risk assessment component suffers from a myopic view of security threats and is more concerned with data security than formal or informal level of organizational vulnerabilities. Measuring the effectiveness of internal controls is a difficult and an ongoing process (Dhillon and Mishra, 2006) and COSO does not provide any feedback mechanism for the improvement of the control objectives.

A review of the research literature in information systems security governance from socio-organizational perspective suggests four emergent themes which are influencing the majority of research initiatives. These themes are a) security policy approach b) life-cycle development approach c) unified approach d) and end user participation approach. Each of

the themes with examples of research being conducted in the particular area are discussed below.

Development and use of security polices for effective governance is heavily researched from socio-organizational perspective of information systems security governance. There have been several calls in information systems security research literature to aid information security policy formulation (Von Solms, 1996; Straub and Nance, 1990). Straub and Nance (1990) use general deterrence theory to facilitate security policy formulation. The objectives of the theory hinge on maximizing prevention and minimizing undetected and unpunished abuse (Straub and Welke, 1998). Moultan and Cole (2003) emphasize the importance of sound security policies as being vital for a security program and provide guidelines for development of internal controls (Cockcroft, 2002, Straub and Welke, 1998). The authors categorize security governance on the following dimensions (see table 2.5): responsibilities in practices, strategies and objectives, management, resource management, regulatory compliance, policies and procedures and external communication. The authors present a comprehensive set of governance principles which have been emphasized in the literature emerging from various quarters over the years.

Table 2.5. Governance objectives (source: Moultan and Cole, 2003)

Dimensions	Objectives
1.	Responsibility in practices
2.	Strategies
3.	Management's role
4.	Resources
5.	Regulatory compliance
6.	Policies and procedures
7.	External communications

The objectives suggested in Moultan and Cole (2003) model are socio organizationally grounded and provide good reference point for developing a governance framework. Inversely, the authors underplay the role of technical expertise required for security governance. Also, the suggested objectives are based on the conceptual understanding of the authors and have no empirical support.

Along the same lines, Eloff and Eloff (2005) suggest a comprehensive approach towards information systems security governance with well managed controls to minimize risk and ensure effectiveness and efficiency. The authors propose a framework called PROTECT, an acronym for the seven components in the model. The components are: *Policy* includes security policies, procedures and standards. It also includes well documented guidelines for implementation. *Risk* component suggests the use of methodologies such as CRAM and Octave for identifying vulnerabilities in the system. *Objective* refers to the main objective of the framework, which is the intention to minimize risk exposure by maximizing security through implementation and review of set of controls. *Technology* refers to the systems component (hardware, software) of the IT infrastructure. *Execute* component refers to proper infrastructure of security controls from maintenance and management. *Compliance* component refers to both internal as well as external compliance with polices and regulations. It comprises codes of practice, legal requirement and international standards. *Team* component refers to the employees' responsibility towards security and aims at creating a work culture with improved security. The model presents both technical and people's "perspective". This model is very high level. The drawback of the model is that there is obvious lack of guidance on how and when to use these objectives.

Security policies, standards and procedures are also highlighted in Information Security Architecture (ISA) model proposed by Tudor (2000). The author defines information security architecture as the process of developing risk awareness through assessment of current controls. ISA also includes the alignment of existing controls to meet the organization's information security requirements.

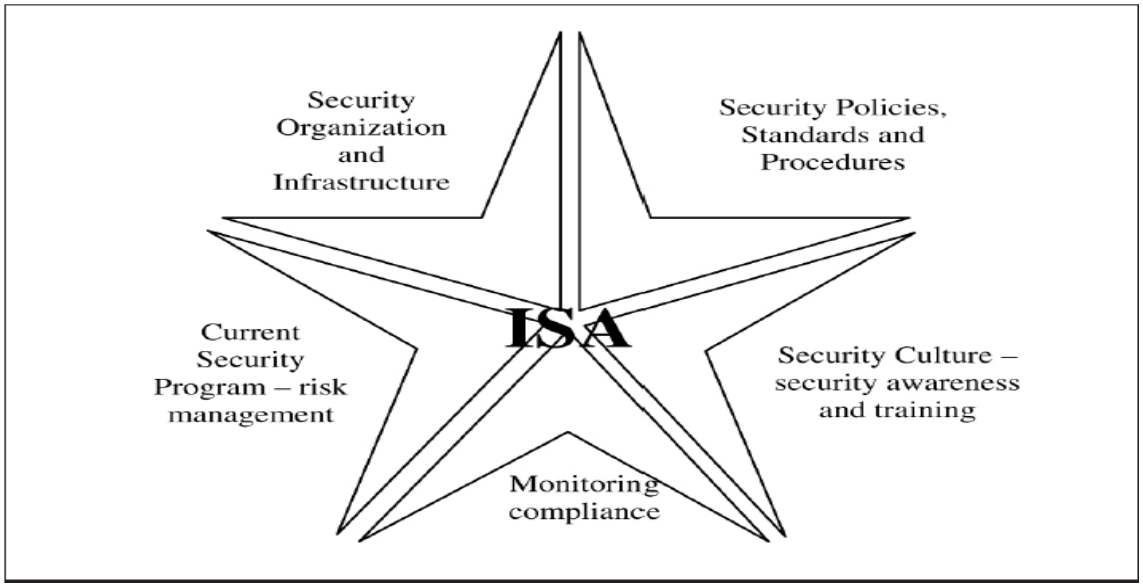

Figure 2.2 Information security architecture model (source: Tudor 2000)

ISA has been conceived as a management process intertwined with day to day operations. In this approach, five key principles are highlighted (see figure 2.2): Security organization and infrastructure, Security policies, standards and procedures, Security program, Security culture awareness and training and Monitoring compliance. The model proposes that all individuals should know their responsibilities with regard to protecting the organization's resources. The architecture is based on a holistic mix of organizational and technical aspects of security governance. The biggest drawback of the model is that it is very high

level, basic, non-iterative and difficult to apply for developing specific measurable security controls.

McCarthy and Campbell (2001) also emphasize the role of security policies in their proposed Capability Maturity Model approach for security governance. The model provides a set of security controls which can be used to protect information assets against harm. The model encompasses seven main control levels (see table 2.6):

Table 2.6. Capability Maturity Model (source: McCarthy and Campbell, 2001)

	Control Levels
1.	Security Leadership
2.	Security Program
3.	Security Policies
4.	Security Management
5.	User Management
6.	Information Asset Security
7.	Technology Protection and Continuity

In the model, *Security leadership* stresses the importance of executive level security representatives within an information security strategy. In the next level, *Security program* provide defined roles and responsibilities for security tasks. *Security policies* which comprise the third level emphasize the use of security standards, policies, and guidelines for technical, procedural and human aspects of information systems security. *Security management* component deals with monitoring people and technology in daily operations. *User management* deals with managing user profiles and ensuring that users are made aware that they are being watched. *Information asset security* encompasses the technology aspects of security i.e. maintain firewall, network and database. *Technology protection and continuity* component maintains the IT environment and its continuity including disaster

recovery aspects. The objective of the Capability Maturity Model approach is to start at a strategic level and work down to the technology level, guided by the direction provided at the top level. The uniqueness of this model lies in its assessment of the current information security capabilities to architect an appropriate security solution. The main criticism lies in the anecdotal nature of the model and lack of theory or empirical validation to lend it credibility.

Security polices are an important component of the information security governance model proposed by Da Veiga and Eloff (2007). The authors propose an integrated information security governance framework which is a result of triangulation of components of many of the above mentioned models. The framework is partitioned into 4 levels namely A, B, C and D. Level A comprises strategic, managerial and technical protection components. Level B consists of six main categories that are grouped according to three levels A categories. Level C is a comprehensive list of information security components categorized under level B components. All the main categories are influenced by change depicted at Level D.

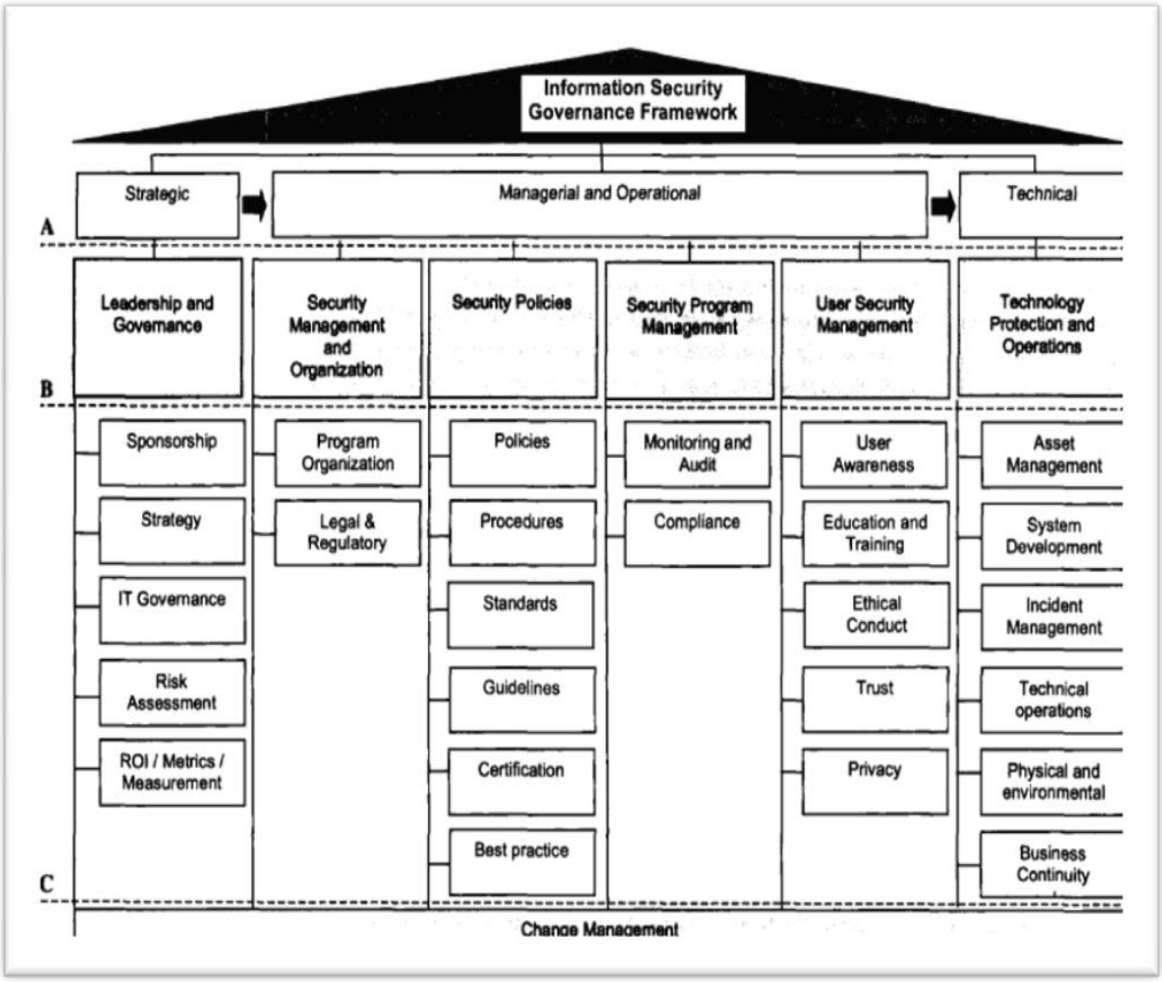

Figure 2.3. Information security governance framework (source: Da Veiga and Eloff, 2007)

The six main categories of this model are (see figure 2.3): Leadership and Governance, Security management and organization, Security policies, Security program management, User security management, Technology protection and Operations. The framework can be deployed as a single point of reference for governing information security. The control objectives listed in the framework provide a wide range of options to protect the organization. The information security management system proposed is based on a common security standard namely BS 17799. The model aims to ensure that best practices

of an organization are documented, reinforced and improved over time. The main benefit of the model is that it could also be used as an information security culture assessment tool to measure the acceptable level of controls consciousness. Action plans can then be employed for areas of development. The model's criticism is that it is based on personal intellectual understanding of the researchers and a thorough review of the literature. There is no empirical work to support or dismiss the importance of the above framework.

The main problem of governance models with a policy focus is the little or no emphasis placed on feedback and modification with changing business requirements. Security polices should be aligned with the security governance objectives. These in turn should be reviewed with changing technological developments (Lindup, 1996).

Rees *et al* (2003) have criticized current approaches to policy development and propose the use of Policy Framework for Interpreting Risk in E-Business Security (PFIRES) model. Initially developed for e-commerce activities, the PFIRES model addresses the needs of security polices for any organization with IT and Internet operations. The framework consists of four stages: assess, plan, deliver and operate. The *assess* stage includes policy and risk assessment whereas *plan* stage involves requirement definition and development of security policy in alignment with business objectives. In *delivery* stage, controls are defined and implemented where as in *operate* stage all control processes are monitored and reviewed. This model emphasizes the importance of feedback in all stages. The main drawback of the model is that it is entirely focused on security policies as a governance mechanism. Security policies are a required but not a self sufficient condition for good information systems security governance.

In the life-cycle approach, the underlying assumption is that information systems security governance is an ongoing process and needs to be viewed from a business process perspective. The models suggested in this stream of research are process based and the stages defined are similar to those of software life-cycle development. The security governance models with requirement analysis, design, implementation and testing have a solid foundation in the systems approach underlying many IS development and management approaches. Some of the examples of process models are presented below: Kolokotronis *et al* (2002) propose a multi-dimensional model with following objectives: business needs or requirement analysis; risk and cost assessment; security strategy implementation and monitoring. The authors suggest that security should be managed at a corporate level and not at the local level to solve specific technical problems. Moultan and Cole (2003) present a similar argument in support of treating security governance as an enterprise issue to establish an adequate control environment. It is important to identify risks so that management can assign responsibility to the right people to develop and implement appropriate controls to mitigate the risk.

Table 2.7 Information security governance objectives (source: Kolokotronis *et al*, 2002)

Number of dimensions	Objectives
1.	Requirements analysis
2.	Risk and cost assessment
3.	Security strategy
4.	Monitoring

Using a similar approach, Straub and Welke (1998) present a security risk planning model that comprises four stages: security problem definition, risk analysis, alternative generation, and planning decision. The authors argue that very little is available in

literature of the present to describe an overall approach to security planning and evaluation process (Straub and Welke, 1998). Both the models discussed above (Kolokotronis *et al*, 2002; Straub and Welke, 1998) have a process orientation to security governance. The models provide high level objectives for defining specific security objectives. The objectives are vague, difficult to implement and not helpful in developing specific information systems security governance objectives and their related controls. The main limitation of the studies is a lack of scientific evidence concerning the practical usability of the results.

In the unified approach of information systems security research, the central premise is that both organizational and technical aspects of security governance should be combined for increasing overall security. The base assumption here is that managerial focus for security governance is required for the technological solutions to work efficiently. Dutta and McCrohan (2002) argue that sophisticated security technologies can be rendered ineffective by the failure to differentiate among critical information assets, poorly designed operating procedures or lax attitudes towards security within the organization.

Poole (2006) argues for an information security framework established by combining the best of ISO 17799 and COBIT into an information security benchmarking model. This model meets the corporate governance requirements by focusing on both the control and accountability framework. The author argues that these benchmarking models are being successfully deployed in UK and across Europe. Dutta and McCrohan (2002) present a security governance model which comprises three dimensions: organization, critical infrastructure and technology. The role of management in this model is to assess the

criticality of data sources and develop controls for the organization. The authors argue that holistic security management requires interplay of technological, organizational and critical infrastructure elements. Hence, awareness and commitment of the senior management is required to develop a control environment that balances the costs and benefits of security controls, keeping in mind the level of risk faced by the organization (Dutta and McCrohan (2002). The model proposed is comprehensive and deals with both technological as well as socio-organizational elements. The drawback of this model is that is based purely on authors' conceptualization. The model is subjective at best and lacks empirical validation.

Along the same lines, Lindup (1996) also argues that the management in the organization does not operate in isolation. The effectiveness of the security governance is dependent on many factors (see figure 2.4) that include: business processes, application systems, technical security, procedures and human factors.

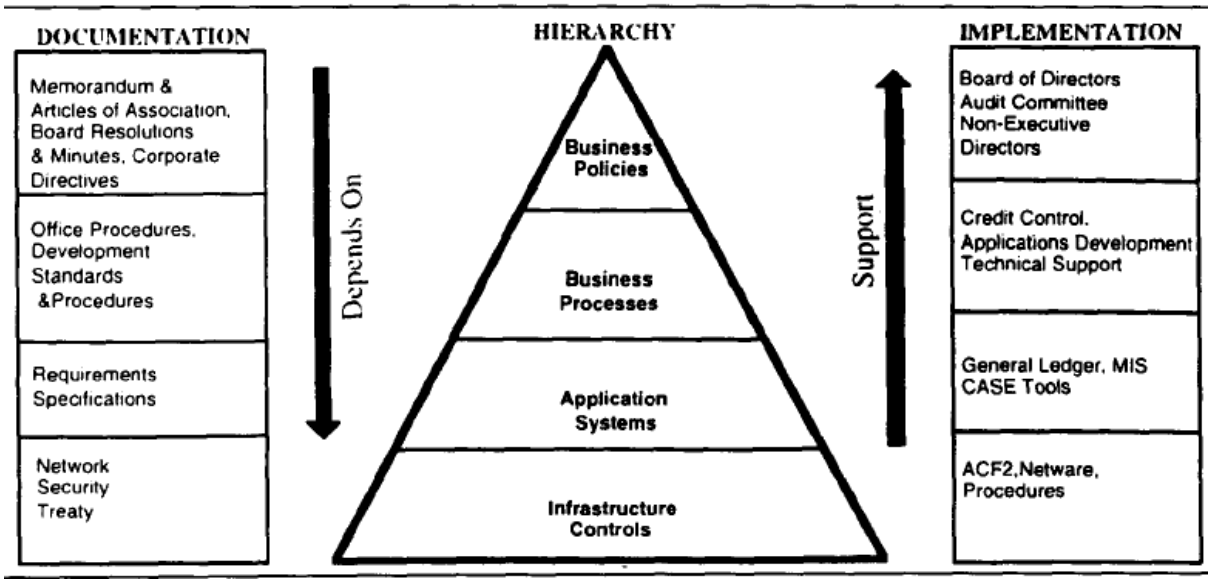

Figure 2.4 information security management model: Lindup (1996)

The emphasis again is on socio-organizational as well as technical issues in governance and on challenges that arise in managing the human capital. The author argues that technology can impact organizational security in unexpected ways. Technology can make existing controls in the higher layers ineffective or make new control mechanisms possible. It can impact security and control in three different ways: creating new security vulnerabilities, changing the way business is done and changing the way the workplace is organized (Lindup, 1996). The pervasive presence of technology in businesses makes it difficult to isolate the technical aspects from managerial aspects of governance. More than the technology, it is "the way a technology is used" that has the greatest impact on the security of the information systems (Lindup, 1996). However, this model too is based on conceptual understanding of the author and not on a solid theoretical platform.

From end user participation perspective of information systems security governance research, control objectives should convey the value and beliefs of the employees actually implementing the controls. The central assumption is that a "bottom-up" approach to development of security governance objectives increases the alignment between individual objectives and organizational security objectives, resulting in organizations which are more secure. The researchers in this domain of security governance research encourage employee participation in governance.

The advocates of this school of thought argue that very few organizations involve end users in development of information security strategy and policy making (Warman, 1992). This might result in making the security objectives too complex and weak controls which would lead to a break down in security (Angell, 1996). Also ignorance or incorrect

procedures can lead to potential disasters (Warman, 1992). In a study in 2002 advocating use of meta policy for security in emergent organizations, Baskerville and Siponen argue that changed security measures should not spark conflict between management and the employees in an organization. When the values of the employees do not match the values embedded in the security measures, there are chances of discrepancies in implementation of such measures (Baskerville and Siponen, 2002). Values are a key determinant of how people come to evaluate other people and organizations (Jones and George, 1998). Schein (1996) claims that organizations do not learn from its experience but tend to repeat the same mistakes made in the past due to a continued lack of alignment between various occupational communities within themselves. This might result in operational and mid-level managers having different shared assumptions and objectives. These will be far removed from the objectives preached and practiced by senior managers. The alignment of personal and organizational objectives for information systems security governance is important for the success of the controls. Technology used is influenced by the values and goals imposed by the executive culture in the organization (Schein, 1996). Taylor (2006) argues that it is management's mistaken perception of risk causing behavior which leads to an implementation of a technology based approach that ignores human factors.

De Haes and Grembergen (2008) argue that IT governance can be deployed using a mixture of various structures, processes and relational mechanisms. Anderson (2001) argues that within IT governance, information security governance becomes a much focused activity, with specific value drivers including integrity of information, continuity of services and protection of information assets. Thus the relational mechanism which

ensures the active participation and collaboration of the IT managers and business managers is equally important for information systems security governance too. The authors argue that relational mechanisms are crucial in the governance framework and paramount for attaining and sustaining business/IT alignment, even when the appropriate structures and processes are in place. Research in management controls has historically emphasized the role of senior management in the success of internal control programs. This trend is now changing. Controls research has shown an increase in interest in employee empowerment (Simons, 1995). It is becoming common for lower level employees to be actively involved not only in day-to-day processes but also in activities of strategic significance.

In conclusion, research in information systems security governance area with a socio-organizational focus can be summarized as follows:

1. Security governance is viewed as an all encompassing process which involves managing formalized structures and informal environment. Hence emphasis is placed on formal as well as informal controls.
2. Security governance models are primarily focused on factors like policy development, management and end user participation, user values and beliefs, life-cycle or process orientation and complimentary nature of various controls or the unified approach.
3. Security controls are based on ‘formal administrative’ management requirements and ‘informal peoples’ management requirement. It is assumed that management,

formal procedures and informal people management mechanisms would ensure the overall security of the organization.

4. It is assumed that management understands the need for appropriate socio-organizational controls and that implementing these controls would enhance the security environment.
5. Information systems security governance models that emphasize on the management's role in creating and developing security governance objectives embedded in the contextual factors of the organization are successful in protecting the organization from any harm.

Since most of the IS security breaches occur because someone within the organization subverts the controls (Dhillon and Silva 2001), researchers in this domain argue that it is prudent to focus on the socio-organizational aspect (Dhillon and Torkzadeh, 2006) of security to provide overall better governance.

2.4 Discussion

The purpose of this chapter is to thoroughly review the extant literature in information security governance research. The research in information security governance can basically be classified as per two dimensions: technically oriented research and socio-organizationally oriented research. It is to be noted that this classification does not convey that proponents of either streams of research are not sympathetic to each other's premises. Researchers do acknowledge the need for both these dimensions. The classification is based on implicit assumptions of the research and the dominance of one orientation over the other.

The fundamental difference between these two streams of research (see table 2.8) lies in the nature of assumptions, nature of controls developed, end user role and the results of using the particular approach for the organization.

Technically oriented security governance research perceives security as managing data in computers. Hence the nature of controls implemented is technical in nature which includes passwords, access control, sniffers etc. The end-users are expected to have the technical expertise to implement the artifact in a way that delivers the intended benefit from the technology used. The final goal of implementing such controls is to build a strong IT infrastructure that protects the network from outsiders. The efficiency also improves as technology related failures are minimized.

Table 2.8. Research in information systems security governance

Technical Vs. Socio-organizational

Dimensions	Technical orientation	Socio-organizational orientation
Assumptions	Security governance is "managing confidentiality, integrity and availability of data"	Security governance is managing formal structures and the informal environment.
Nature of controls	Technical	Formal and informal
End- user role	Technical solutions are well understood Implementation would give intended benefit	Need to understand and participate in control development process Understand responsibility and control culture
Result	Strong IT infrastructure Better protection from outsiders Reduced technology related incidents	Strong management and people interaction Better protection from insiders Greater acceptability of controls

Research in socio-organizational orientation conceptualizes governance as a process of involving all stakeholders and assigning responsibilities in a way which makes information systems secure at the formal and informal levels of the organization. The nature of controls suggested are both formal and informal. End-users in the organization are required to

participate in the control development process and understand both their responsibility and the control culture of the organization. The ultimate goal of such measures is to make controls more acceptable, improve management and end-user interaction and protect the information systems from insiders.

A review of research from both the perspectives reveals various facets of using these approaches. A summary of the findings from the review of both perspectives is presented in table 2.9. Before each body of work is discussed separately, an overall critique of industry wide standards or best practices utilization is presented. As we have seen in the discussions above, COBIT, COSO, ISO 17799 and ITIL are some of the common standards used extensively in the industry and supported by different groups of researchers. Standards provide a set of best practices across industries and are helpful in getting the work done efficiently in real organizations. But these standards are not without drawbacks. Several issues arise when the general standards are used "as it is" by the organization. First, security standards are generic in nature and do not reflect the unique security requirements of an organization (Baskerville, 1993). Second, standards do not take into account the social nature of governance problems (Dhillon and Backhouse, 2001). Third, the standards are not adaptive in nature and do not suggest courses of actions in the event of changing business requirements of an organization initiating ad hoc managerial decision-making and judgment (Ferris, 1994). Standards are not based on any theoretical platform or developed using rigorous research standards. These standards do not add to the body of knowledge in research.

In technically oriented information systems security governance research, bulk of the research has been done in systems dominated requirements such as information security architecture, access controls, Internet usage, network protection and database controls. Majority of work in this domain (Abouzakhar and Manson, 2002; Qiang and Hua-ying, 2007; Finne, 1996; Booker, 2006) argues for a solid technical foundation for security of information systems by developing capabilities for strong IT infrastructures. These will facilitate the management of technical controls as a centralized function. The drawbacks of research from this perspective are based on the fact that it does not adequately address vulnerabilities from the "inside" i.e. formal and informal issues with security management. Also, security management frameworks with technical emphasis are "standalone" in nature and cannot be easily combined with other frameworks for enterprise wide governance of security.

Technically orientated information systems security governance models are unable to fully comprehend several behavioral complexities that may need to be resolved to enact security solutions. Research in information systems security area is predominantly technically oriented (Dhillon, 2001). It is not surprising that many of the security governance models too are rooted in technical foundations. But having a predominant technical orientation does not lend itself well to incorporation of in-depth feelings, emotions, attitudes and perceptions toward security. A sympathetic understanding of the contextual formal and informal issues is required for an overall successful governance program. Information security is not just a technical problem but has several other facets to it just like leadership, culture and structure (Dutta and McCrohan, 2002; Da Veiga and Eloff, 2007). Similarly

information systems security governance objectives can not be just technically oriented to provide a comprehensive security program. In socio-organizationally oriented information systems security governance research, majority of the work is confined to the area of development of policies, end-user participation, iterative process orientation and unified approach combining formal and informal with technical controls. Research in this domain (Ward and Smith, 2003; Moultan and Cole, 2003; Eloff and Eloff, 2005; Tudor, 2000; McCarthy and Campbell, 2001; Da Veiga and Eloff, 2007; Rees et al., 2003) argues for aligning individual and organizational security goals and combining formal and informal controls with technical controls for a comprehensive security program. There are several benefits of using governance models rooted in this perspective. Vulnerabilities from "inside" are addressed and the organizational environment becomes more conducive to security practices. Incorporating values from end-users or using a "bottom up" approach to governance suggests better implementation and success of these controls. There are some drawbacks as well of using these models. Most of the frameworks suggested are "anecdotal" in nature i.e. based on practices, experience and understanding of the researchers. There is hardly any model with security governance objectives which has been empirically tested for its applicability and usability in real organizations. Also different proposals and examples of security governance objectives do not provide guidance with respect to the process of objective development.

Table 2.9. Summary from literature in information systems security governance

Perspective	Exemplar work	Implications for security governance	Pros & Cons
Technically oriented research	-ISO 17799 (2007) -ITIL (2007) -Abouzakhar and Manson (2002) -Qiang and Hua-ying (2007) -Finne (1996) -Booker (2006)	- develop infrastructure to ensure confidentiality, integrity and availability of data -establish information systems security architecture -develop stringent access control models -establish means to protect networks - emphasize Internet security - emphasize database security -ensure identity management -ensure incident management	- solid technical foundation for securing information - develops capabilities to maintain efficient IT infrastructure -integrates enterprise wide technical security controls into a superior centralized function - "standalone" in nature, not easily integrated in governance framework -develops vulnerability in organization's formal procedures and informal people management aspect
Socio-organizationally oriented research	-COBIT (2007) -COSO (2007) -Ward and Smith (2003) -Moultan and Cole (2003) -Eloff and Eloff (2005) -Tudor (2000) -McCarthy and Campbell (2001) - Da Veiga and Eloff (2007) Rees et al. (2003) - Kolokotronis *et al* (2002) - Dutta and McCrohan (2002) - Lindup (1996) -Anderson (2001)	- formal controls at management level and informal controls for people management are more important than technical controls for security governance -develop sound security policies -perceive security governance as a process of system development and develop iterative approach to improve it - develop a unified approach to governance combining technical as well as socio-organizational controls -incorporate individual's values and encourage end user participation for security governance	-vulnerabilities in form of management lapses and people management issues can be avoided -continuous feedback to improve control objectives improves governance results - incorporating technical and non-technical controls in governance models improves overall security -better alignment of individual and organizational goals -high level, generic objectives are difficult to implement -"anecdotal" models based on conceptual understanding. Lack empirical support

Socio-organizationally oriented information systems security governance research emphasizes the importance of formal procedures and informal aspects of the organizational environment. Interactions between stakeholders have also been discussed at the level of

information security governance. Security governance models in this domain emphasize the management's role in creating and developing security governance objectives embedded in the contextual factors of the organization. As Dhillon and Torkzedeh (2006, p. 17) observe:

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, 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 complete 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.

Managing security is also problematic because employees are unaware of the appropriate security policies and standards (Ward and Smith, 2002). Understanding perceptions of an organization's board members and other stakeholders with regard to risks and market expectations is crucial to improving Information Security Governance (Ezingeard *et al*, 2003). Since most of the IS security breaches occur because someone within the organization subverts the controls (Dhillon and Silva 2001), it is prudent to focus on the socio-organizational aspect (Dhillon and Torkzadeh, 2006) to manage security in a better way.

A review of information systems security governance research shows many apparent gaps in the literature. First, research from technical perspective provides good technical basis for managing security but is not sufficient by itself to provide comprehensive security.

Second, research from socio-organizational perspective undermines technical perspective and most of the models suggested have not been empirically validated in real settings. Third, participative approach of governance which proposes involving the values of end-users in governance is discussed in the research but there is hardly any work done in this area. There is a dearth of models that incorporates end-user inputs into governance objectives. Fourth, there is hardly any research that suggests how to develop the security governance objectives i.e. what process to use or what methodology to follow. Fifth, there is very little work based on theoretical foundations. Most of the models are based on conceptual understanding and experience of researchers. More research is required to address the gaps identified in information systems security governance research. This research addresses some of these gaps by developing organizationally grounded value driven information systems security governance objectives that are theoretically sound and empirically validated.

2.5 Conclusion

Technical and organizational perspectives of information systems security governance offer different prescriptions for implementing security controls. The technically oriented models emphasize specific problem selection, tool selection and knowledge acquisition about the tool to solve any problem. A review of the research shows over-dependency of the organizations on the availability of technical tools to manage security problems. The socio-organizationally oriented models, on the other hand, emphasize the need for managing formal security policies development processes, management of individuals and creating an environment to facilitate the security

management. Both organizational and technical orientation is required for overall security of the organization. The challenge lies in prioritizing the objectives and allocating adequate resources for the fulfillment of both types of objectives.

The goal of this chapter was to present an in-depth review of various information systems security governance approaches in literature. In the beginning of the chapter, the research literature was divided into two distinct streams: technically oriented governance models and socio-organizationally oriented governance models. The assumptions and differences between the two approaches have been established. Having identified the potential benefits and drawbacks of using governance models from both the perspectives, this chapter discussed various noticeable gaps in the research of information systems security governance. The discussion section suggested a gap in the research in the area of developing theoretically grounded value based information systems security governance objectives. This gap will be addressed in this research. The following chapter outlines a theoretical basis that helps in developing value based governance objectives for information systems security. The assumptions of the theory will be explained followed by a brief review of use of values in information systems research and information systems security research. The methodology to develop the objectives would be discussed and substantiated.

CHAPTER 3 Theory and Methodology

3.1 Introduction

This chapter describes the theoretical and methodological foundations of this research. The theoretical and methodological position of a study must be consistent from a philosophical perspective. The ontology, epistemology, methodology and the methods used in a study should be consistent to qualify as a valid research design. Since this study uses individual values to develop ISG objectives, an introduction about research in individual values is warranted. Rest of this chapter is organized as follows:

The following section presents a synopsis of the existing research in individual values in IS and the pertinent lessons which have emerged for studying values in ISG. After establishing the importance of values for ISG, the following section presents a discussion on 'Value Theory as a theoretical platform' with reference to this research. The methodological position of the study is explained in section three of the chapter. Section four outlines the research design for the study. The last section presents the conclusions.

3.2 Study of values in research

This section presents a discussion on the use of "values" in information systems research. The discussion is presented in three parts. First part presents a holistic preview of how values have been studied in information systems security research. Second part presents a discussion on how values have been used in research in the management discipline. Third part presents the lessons derived from using values in information security governance research.

Concept of values in IS Security Research

Research in information systems security recognizes the importance of individual values in successful security programs. Solms (2001) specifically mentions the fact that information systems security policies and controls in general do not have human considerations. Successful implementation of the controls and polices is facilitated when individuals are able to align their value system with that of the management. Researchers argue that if there is a misalignment between individual and organizational goals, there will be greater security threats to information systems from the insiders in the organization (Loch and Conger, 1996; Solms, 2001; Magklaras and Furnell, 2005; Stanton, 2005). Dhillon and Torkzadeh (2006) study the significance of values of employees for information systems security in organizations. The employees should be treated as owners of information assets (Adams and Sasse, 1999) to ensure that responsibility and accountability, on the employee's part is enhanced.

Concept of values in organizational research

Organizational research has long emphasized the importance of studying personal and group values in organizational settings. Davis (1958) calls management philosophy as the philosophy of individualism and claims, "Management philosophy emphasizes the concepts of delegation, decentralization, individual initiative and individual accountability (p. 39)'. In a study to understand the impact of personal values on organizational decisions, Senger (1971) measured personal value orientations by using a value scale. The values provided the structure for the scale and a semantic differential technique was used as a scaling device. Senger's study suggests that "Personal value structures and systems of preference ordering used by decision-makers could lead to more useful decision models

which are better able to predict choice behavior (p. 422).” Research in authority of management in organizations also studies value systems of individuals. Authority depends on its acceptance by those it intends to direct. Hence any emerging pattern of authority must be consistent with the values of individuals it is directed at and address the emerging ideals, purposes and values of these individuals (Albanese, 1973). A manager’s effectiveness is determined by his ability to synchronize the values of his associates and the pattern of authority he attempt to implement (Albanese, 1973).

Lessons for studying ISG

Information systems security research fully acknowledges the importance of individual values in security posture of organizations. Individual beliefs of employees shape the interpretation and hence the success of all security measures in an organization (Magklaras and Furnell, 2005; McHugh and Deek, 2005). Importance of normative controls in an organization has been emphasized in information systems security literature. The informal controls help in effectively reaching out to people and conveying management’s ideas (Adams and Sasse, 1999; Schultz, 2002). Assessment of individual values, beliefs and attitudes could be used for predicting employee’s attitude and behavior (Stanton and Stam, 2005). Employee’s behavior, especially for security issues, is critical for an organization. User sophistication, social engineering and end user behavior are well-researched constructs in security literature (Loch and Conger, 1996) and the findings emphasize the importance of individual belief systems in security management.

A thorough review of research in the previous chapter suggests that the designing of ISG lacks appropriate theoretical basis and there is a need for more investigation of issues in

this area. Weber (1997) argues for more theory building efforts in information systems is needed to increase legitimacy of research in the discipline. Taking phenomenon that are purportedly forwarded and accounted for by theories from other disciplines and building novel theories on their basis to explain information systems issues helps the information systems discipline (Weber 1997). Value theory, borrowed from sociology, provides an appropriate theoretical basis to incorporate individual values into the designing of internal controls for security. Studying individual values in the context of information security governance, helps in creating more effective security programs for organizations. Internal controls depend on the information security objectives of an organization (Haara and von Solms 2003) and should be designed keeping in mind the specific security needs of a particular organization. Internal values of employees can be elicited to establish the security objectives of an organization. Employee's security behavior depends on his personal values and standards of conduct (Leach 2003). Information security governance objectives, which are rooted in personal values of employees, would lead to more robust and proactive design of internal controls. This would bring the security behavior of the employees in accordance with management's expectation, conveyed through internal controls. Employees can relate to the controls (being a reflection of their own core values) and information systems security program can be better governed and implemented.
The benefit of using individual values to develop control objectives is twofold: First, there will be a better alignment between individual and organizational goals if the control objectives are created in a "bottom up" manner. This way of communication can reduce the gap between management expectations and employee interpretations about the

controls. Second, it will facilitate the creation of an environment of shared goals amongst employees, which has beneficial long-term implications for an organization's information systems security. In this chapter we posit that value theory and value focused approach provide an appropriate theoretical and methodological basis to design internal control objectives for information systems security in organizations.

3.3 Theoretical basis: Value Theory

Catton (1952) proposed a theory of value which essentially suggests that the core values of individuals guide their decision making process. According to Catton (1952), an individual's preferential behaviour shows certain regularities and this pattern can be attributed to some standard or code, which persists through time. Values provide a basis by which people can control their intensities of desiring various desiderata (something desirable). Based on available choices, people make preferences or choices which are grounded in their values. In the organizational context, knowledge of such preferences of individuals provides a context for managerial decision-making.

Value is not a property of an object but is a quality of relationship (Catton, 1952, pp. 108). A person's desire for something under a given situation depends upon the "selective perception" of that person. Selective perception directs valuation by interspersing final goals with other intermediary goals i.e. a goal may be pursued in order to attain some higher ultimate goal. Thus the nature of the major goals accepted by individuals is complimented by their notions of ways in which these goals might be affected by future events. These in turn are the determinants of values of people. Value Theory provides a theoretical platform to affirm that values are important for decision making and

incorporating values in developing decision objectives significantly helps individuals accept the results of such decisions.

Catton adopts a field concept of values for understanding and predicting human behavior from studying of values. In this approach, the concept of value is perceived as somatic (in brain) which surround the value object (Catton, 1952). It is assumed to have a correspondence to some postulated external field. The nature of this value field is multi-dimensional. Psychologists have studied values extensively but more in terms of "motivations" (Catton, 1952). However, there is an intrinsic difference in what sociologists call "values" and the psychologists call "motivations". The idea behind studying motivations in management, both internal as well as external, has been the same as in the field of sociology i.e. predicting the human behavior from the study of these concepts. Psychologists argue that human nature does not allow the valuation of anything that is readily available and indispensable to their survival (Catton, 1952). Maslow (1943 in Catton 1952) shares similar views and argues that a readily satisfied need can never motivate human behavior.

Catton conceptualizes valuing as field of forces. He argues that when we observe a person valuing something, certain things become apparent from the behavior of that person. This is true even for various persons at different times in relation to various objects. Based on extant literature, Catton created a comprehensive list of various dimensions of values. The seventeen dimensions of values as studied by Catton (1952) are descriptive of the vast field of valuation: Intensity, Duration, Probability, Permanence, Continuity, Proximity (spatial, temporal, social), Conduciveness to survival, Inclusiveness (of persons, of other values),

Irrevocability, Congruency with other values, Cognitive completeness, Free selectibility, Infinitude and Subsidization.

A multiplicative combination of these measures or some function of each one of these would help in specifying the "worth" of its desideratum to the subject (Catton, 1952). Catton hypothesized the relationship of these dimensions, which impact the values of individuals and empirically studied the hypotheses. According to this theory, the value of a particular object to a particular person, under particular conditions of time and place is specified by the product of the above-mentioned seventeen dimensions raised to some power. Catton (1952) defines behavior valuing as "willingness to give or do something in order to get or keep something else (p. 172)".

The importance of societal conditioning in shaping one's value-attitudes has been amply researched in the field of sociology. Hobson (in Catton, 1952) suggests that "man is made and sustained by association and the process of civilization is nothing else than the progress of the arts of association. In any estimate of human welfare it is, therefore necessary to take our stand firmly on the principle of the social determination of values (In Catton, 1952)". Catton (1952) suggests that any study of a theory of value is meant to persuade people that certain norms or? code of conducts are more acceptable than the others. Values are merely products of some code of behavior, which the advocate of the code wants to propagate. Theories about values enunciate some broader values to which other values might be subordinated. Cooley (in Catton, 1952) defines values as "a special attribute awarded to those objects and ideals capable of serving purposes arising out of needs…that is to say, value is instrumentality (p. 98)". The social nature of the

determinants of value is studied by psychoanalysts as well. Morton observes that time is an important determinant of values and immediacy of interests clouds the judgment of humans in many instances. Extending this time perspective about values, Frank (in Catton, 1952) suggests that individuals, as they mature with time in a social setting, tend to get socialized and start understanding the values of the particular setting. Values are arranged according to different rank orders for different people and this differentiation impacts the sociological analysis of inter-group relations (Catton, 1952). In management science, this concept of values guiding the decision making process was taken forward by Keeney (1992) who argues that values are guiding principles to evaluate the desirability of a particular consequence. "Values are what we care about and they should be the driving force for our decision making (Keeney, 1992, pp. 3)". Values are principles of evaluation, which we use to evaluate the actual or potential consequences of action and inaction of decisions (Keeney, 1992). Focus on values guiding the decision situation makes the search for alternatives a creative process and produces unique alternatives. It expands the horizon of options available to a decision maker by basically answering the question "what is important to me" rather than the constrained thinking of "what can be done" under given constraints. This research uses Value Theory as a platform to guide the study of values in the context of information security governance.

3.4 Methodology

This is a two phased study. Phase 1 of the study uses value focused assessment as the methodology. The second phase of the research uses interpretive case study as the basis for

the research study as the basis for the research. This section provides a discussion on both the methodologies.

3.4.1 Value focused thinking

Research in decision sciences essentially suggests two broad approaches to decision making (Keeney, 1992): Alternative Focused Thinking (AFT) and Value Focused Thinking (VFT). Values are more fundamental to a decision context than the available alternatives. But in common practice, decision-making usually focuses on the choice most desirable among existing alternatives. The relative desirability of the consequences can be best understood if the values of the decision maker are reflected in the decision. Ideally, values should be fundamental to a decision problem, and not the alternatives. Alternatives should be used as a means to achieve the fundamental values. Value focused thinking approaches a decision problem by looking for the best possible solution and working towards making it a reality. Alternative focused thinking considers what is readily available and takes the best alternative from available options (Keeney, 1992).

Keeney (1992) suggests that VFT is a preferable way of taking decisions especially if there are lots of subjective interpretations involved. Alterative focus thinking, even though very popular for decision making in day-to-day life, has several shortcomings (Keeney, 1992). AFT has a narrower focus than VFT. The former aims to solve decision problems whereas the latter is concerned with the identification of decision opportunities, which is more of problem finding (Keeney, 1992). Alternative focused thinking is more reactive in nature. Value focused approach leads to best possible consequence that helps in identification of

decision opportunities. It is proactive in nature, affirmative and helps in developing decision objectives for the problem context.

An objective is a statement of something that one desires and is characterized by three features (Keeney, 1992): a decision context, an object and a direction of preference. To be more specific, if the decision context is the development of information security governance objectives, the object would be effective information security governance and the directional preference would be positive i.e. more information security governance is preferred over information systems security.

Fundamental objectives are useful for the purpose of creating and evaluating alternatives, identifying decision opportunities and guiding the decision making process (Keeney, 1992). Desired properties of fundamental objectives include (Keeney, 1992):

- *Essential:* The objectives should be able to indicate consequences in accordance with the basic reasons for interest in the decision situation. Depending on how essential the objectives are, decision context is influenced greatly by these objectives.
- *Controllable*: The objectives should be able to adequately address the consequences that are influenced only by the choice of alternatives in the decision context and not by other confound variables beyond the decision context. It requires a balancing act to reach the right degree of essential and controllable mix in the objectives chosen.
- *Complete*: The objectives should include all possible aspects of the consequences of the decision alternatives. The knowledge of the possible consequences with

respect to each alternative provides a list of all the implications of interest when a particular alternative is selected.

- *Measurable*: The objectives should be defined in such a precise way that even the degree to which an objective can be achieved could be measured.
- *Operational*: The objectives should be operationlizable for an analysis in conjunction with the time and effort available. It should fully address whether it is possible to obtain the relevant information useful for thinking and analyzing the consequences.
- *Decomposable*: The objectives should be such that a separate treatment of each of the objectives should be possible. Aspects of consequences relating to one attribute can be treated independently from aspects of consequences of other attributes.
- *Non-redundant*: The objectives should reflect unique alternatives for different possible consequences. Double counting can occur in two ways: possible impacts of the alternatives and values of those impacts.
- *Concise*: The number of objectives should not be too many. This can help in crating a parsimonious model. This requires omitting any objective that is not deemed useful. An objective should be omitted from the list if various alternatives can be differentiated in terms of that objective. If including the objective has no impact on the relative desirability of the alternatives, it should not be included.
- *Understandable*: The objectives should be able to facilitate generation and communication of insights for guiding decision-making process. It should be

adequately understood by individuals who are in positions to make or influence decisions.

The decision context and fundamental objectives together provide the decision frame (Keeney, 1992). The decision context defines a set of alternatives necessary for a specific decision situation. The fundamental objectives explicitly identify the core values of a decision context and define the consequences which are of concern. It also identifies the essential reason for interest in decision situation. Thus fundamental objectives are the end objectives and the means objectives help in achieving these fundamental objectives. Means objectives have implications and aid in achieving the fundamental objectives. It is important that decision context and fundamental objectives are compatible as they are interdependent (Keeney, 1992). In the figure 3.1, these concepts are shown.

VFT provides a method to elicit the individual values necessary for creating a common denominator of a multi criteria decision-making context. Keeney (1992) proposes semi structured interviews as one appropriate method of collecting data in this methodology. According to the value focused approach, the best way to understand underlying values about any issue is to ask people what is important to them in a particular context and the reasons why they deem it important (Keeney, 1999). For a particular research problem, personal values of people regarding the research question are elicited. Keeney suggests a three-step process for using value-focused approach in an inquiry. These steps are:

Elicit and create a comprehensive list of personal values underlying the problem: The aim of the researcher at this stage is to elicit the underlying values of respondents through probing. The process of identifying the values begins with interviewing people. An

explanatory definition is provided about the research context, scenarios are projected and interviewees are asked to provide examples to demonstrate their choices. Direct questions about values might not be useful as values are difficult to bring to surface and are more difficult to express explicitly. The personal values which are projected during the interview session are listed.

Obtain a common denominator or common objectives: a list of objectives corresponding to the values of respondents is generated at this stage. The data collected (transcripts of the interviews) are converted into a common form at this stage. These common denominators give rise to values. The values thus generated need a verb to generate the objectives. The values that are listed are objects and ways to achieve this object becomes the objective. The verb form of the values thus created could be termed as the objective of that object.

Classify the objectives as fundamental for decision context or as means objectives: this is the final step in value-focused approach which leads to the end result of a network of means and fundamental objectives. Classification of all the objectives formed is done and the objectives clusters are divided into two categories, "means" or "fundamental". Depending on the role of a category in a decision context, a category can be relegated as "means" to the decision or an "end" to the decision objective for the particular problem context. An objective that leads to another objective being considered in decision-making is a *means* objective whereas an objective which is fundamental and important in its own right in a decision making process is called *fundamental* objective. Differentiation between means and fundamental objectives is primarily done through performing a Why Is This

Important (WITI) test for each of the objectives (Keeney, 1992). The entire process depicting the development of control objectives from the values is shown in figure 3.1:

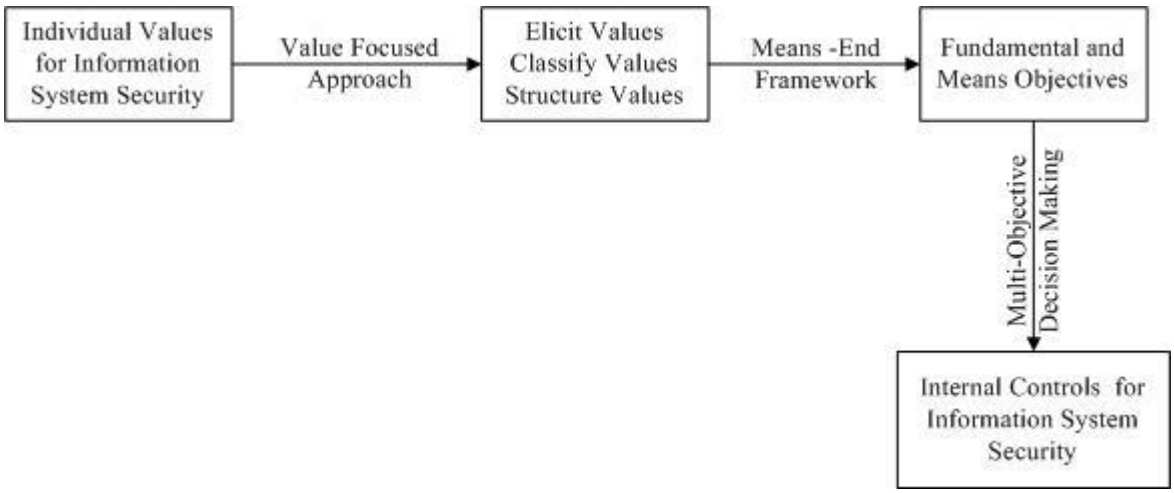

Figure 3.1 An overview of using VFT to generate decision objectives

3.4.2 Case study

This research adopts an in-depth case study approach. This qualitative in-depth case study is performed to interpret the meanings of the objectives in an organizational context.

The choice of case study as a methodology in the second phase of the study is based on the reasons suggested by Benbasat et al (1987). The authors argue that a field case study helps in presenting a rich picture of the phenomenon under study without disturbing the natural state of entities. The relevance of the developed objectives needs to be studied in a real organizational setting to bring out their meaning fully. In a natural setting, events unfold in relation to the focus on contemporary issues and this makes a realistic picture of the relevance of the constructs under study emerge.

For establishing the rigor criteria, this study uses the seven principles of Klein and Myers. Klein and Myers (1999) propose seven principles for conducting interpretive field work. The interpretive field studies in information systems research have repeatedly referred to these guidelines for conducting the research. The first principle, the fundamental principle of the *hermeneutic circle* suggests that human understanding is developed by iterating between the interdependent meaning of parts and the whole they form. This process of constituting the whole picture from constituent parts is fundamental to all the principles proposed. An illustration of the principle is evident in Lee's (1994) study of information richness in email communications. Lee constructed the global context of the email exchanged in the organization and interpreted the meanings of the fragments of the messages exchanged through email. The principle of *contextualization* needs incorporation of the critical reflection of the social and historical background of the research setting. This helps in presenting a coherent picture about how the current situation under investigation emerged. The principle of *interaction* between the researchers and the subjects requires a clear projection so as to bring out how the research materials were socially constructed through the interaction between the researchers and the participants. For example, Trauth (1997) explains how her understanding improved as she became self-aware and started to question her own assumptions.

The fourth principle is of *abstraction and generalization*. This principle is about relating the idiographic details revealed by the data interpretation through the application of hermeneutic circle and contextualization of the data, to theoretical concepts that describe the nature of human understanding and social action. The principle of *dialogical reasoning*

needs openness towards possible contradictions between the theoretical preconceptions and actual findings at the case site to be adopted. This reasoning process leads to subsequent cycles of revision and a modified interpretation emerges. The principle of *multiple interpretations* is about the possibility of differences in interpretation of the participants responses as expressed in multiple narratives or stories of the same sequence of events under the study. The seventh principle is about *suspicion* that requires sensitivity to possible biases or other distortions in the narratives taken from the respondents.

In literature, choice of case studies for empirical research is criticized for lack of statistical generalizability. This criticism is unfair. There have been several responses in literature to counter argue this perception. The choice of methodology should be based on the ontological and epistemological stance of the research. If one views the social world objectively, then the methodological choice should be quantitative techniques. But in this research, social world is viewed as a subjective reality. Hence a qualitative and interpretive approach to research is advocated and in-depth case study is an optimal choice here. As Walsham (1993) argues:

> From interpretive position, the validity of an extrapolation from an individual case of cases depends not on representativeness of such cases in statistical senses, but on plausibility and cogency of the logical reasoning used in describing the results from the cases, and in drawing conclusions from them (p.15).

There is a common misconception that qualitative case studies' results lack usefulness due to the results being statistically generalized from a sample to a population. The argument is that since the sample size is very small in case studies (in a single case study it is one) hence no meaningful statistical technique can be applied to the data. But this criticism

seems unwarranted given the nature the case studies. According to Yin (2003), cases are not sampling units and should not be chosen for this reason. If they are not sampling units, then they should not be analyzed or generalized in a statistical manner.

Lee and Baskerville (2003) argue against statistical generalizability, claiming that it is actually a form of inductive logic. The authors argue that to establish statistical generalizability, we need to follow an additional premise. This is the 'uniformity of nature' assumption which forwards the view that the future would be like the past. Since the principle of uniformity of nature cannot be satisfactorily established, the relevance of statistical generalizability is questionable. One would have to continually regress through the circular logic of the Uniformity of Nature in a vain attempt to validate inductive logic (Lee and Baskerville, 2003). This problem of induction is credited to an 18th century philosopher Hume, and is sometimes called *Hume's Truism*.

Yin (2003) argues that generalization of results, from either single or multiple designs, is made in reference to theory and not to populations. He contends that multiple cases do strengthen the results of the research by replicating the pattern matching. Replication can increase the confidence in the robustness of the theory but by no means does it increase the generalization of the results to entire populations. There are examples of cases studies which go beyond the statistical results and explain the situation from the perspective of human actors involved. These case study evaluations cover both process and outcomes as this methodology can include both quantitative as well as qualitative data.

There are several examples of the use of case methodology in the literature. Yin (2003) has listed several examples of case studies along with the appropriate research design in each

case. Yin (2003) suggests three types of case studies: exploratory, explanatory, and descriptive case studies. According to Yin, each of those three approaches can be either single or multiple-case study, where multiple-case studies are replicatory in nature and not sampled cases. In exploratory case studies, fieldwork, and data collection may be undertaken prior to definition of the research questions and hypotheses. This type of study has been considered as a prelude to social research on a particular topic. This type of case study requires that the framework of the study must be created ahead of time. Results from pilot studies can be useful in determining the final research design. Selecting cases is a difficult process, but the literature provides guidance in this area (Yin, 1989). Stake (1995) suggests that selection should be based on opportunity to learn about the problem, and subjects should be willing. A selected case generally represents a typical environment conducive for the problem. Explanatory cases are suitable for doing causal studies. In very complex and multivariate cases, the analysis can make use of pattern-matching techniques. Descriptive cases require that the investigator begin with a descriptive theory, the findings for which are in the form of in-depth description of the phenomenon from the researcher's perspective. Each research strategy has advantages and disadvantages. Yin (2003) suggests three conditions on the basis of which a research strategy could be designed. These are: nature of research question, the control a researcher has over actual behavioral events and the focus of the researcher on contemporary vis a vis historical events.

In this study, the field case study took place from October 2007 - April 2008 in the Department of Information Technology for the City, a major south eastern city of USA. The data collection and analysis methods are discussed in the next section. The specific

data collection methods will be discussed in the following section. The entire staff of the IT department (with particular attention being focused on the IS Security policy group) was interviewed. The IT department totals approximately 100 employees. Daily observations and intensive document review will accompany these interviews.

3.5 Research design

3.5.1 Data Collection

This research was conducted in two phases. Phase one used value focused thinking and phase two used in-depth case study as a methodology. In data collection for phase one, which used VFT, 52 interviews was conducted with a diverse group of people representing a good mix of people from the various functional areas of different organizations. From the security side, we have representation from Chief Executive Officer (CEO), Chief Information Officers (CIO), information technology directors, security managers, security officers, system administrators, systems auditors and helpdesk IT specialist. We also interviewed people with non IT job specialization for a fresh perspective about security controls. These respondents were manager and line staff from functionalities other than IT such as accounts, finance and human resources. The interviews were conducted over a period from July to November 2007. The average duration for the interview was 45 minutes. The interviews were mainly semi-structured but a question template was developed to guide the discussions. The template is attached in appendix 1. The conversations were tape recorded and transcribed personally by the investigators. Participants in this study represent nine industries and provide a wide perspective on security governance issues. The industries included in this study are: Insurance,

healthcare, credit card services, Banks, financial investment, energy, telecommunications, Internet service providers and real estate development, both in private as well as government sector. The respondents had at least 5 years of professional work experience and have significant experience of using IT and all are under the purview of security governance practices. Some of the respondents do not directly work in information security governance domain but were nonetheless included in the study. We feel that the pervasive nature of security controls impacts everyone across the board in an organization and it is useful to get the values of even those people who were not directly responsible for developing and implementing these controls.

For data collection purposes in phase two of the study, which was an in-depth case study, a number of sources of data were used. Primary source of data was the semi structured interviews. Secondary sources include the policy and procedure manual, the audit manual at CCIT, the policy guidelines provided by the state agency which is responsible for the security policies of the state for the case study, primary source of data was the interviews with organizational members. Key stakeholders were identified at the case study site with the help of our point of contact at the organization. The key stakeholders were able to provide adequate insight into organization's internal control structure in the context of information systems security. The target organization has 4 main divisions: IT development, IT infrastructure, Security and Project management. Each division head and the manager from the particular department were interviewed. The CIO of the organization and the chief audit officer were interviewed increasing the total number of interviews to 10. The overall representation of the respondents (top management, middle management

and operational level) provided good insights into the applicability of the developed objectives in the particular organizational context. See appendix 2 and 3 for the topic guide used in the interviews and list of the respondents. Notes were taken during the interviews and were recorded in the master response document as soon as possible after the meetings.

3.5.2 Data analysis

For data analysis of phase one, we used Kenney's three step methodology to develop the decision objectives (explained elsewhere). For the data analysis of the case study in phase two, several methods were used. Huberman and Miles (1994) suggest three ways of data analysis for qualitative interview data: data reduction, data display and conclusion drawing. In data reduction process, the researchers identify portions of the data which is relevant for the theoretical construct under study. With the useful data, the researchers categorize and structure the data in a manner to facilitate the drawing of meaningful interpretations. This is done through writing summaries, synopsis or making networked diagrams that permit conclusions to be drawn. Finally conclusion drawing is the interpretive process through which the researcher analyses themes and patterns and then compares and contrasts these to triangulate the data. Walsham (2006) suggests that even though the researcher is the agent of the interpretation, a theoretical framework should be used to guide and bind the researcher. Else, the result would be more anecdotal than empirical in nature. In this case, each of the above three steps were performed iteratively several times before actual results emerged. When the initial set of results did not seem to provide insightful conclusions; the entire process was repeated. Various issues were

identified during the data analysis from the primary and secondary sources. Several iterations took place before the objectives were put into clusters. These clusters were revisited with the second phase data and many of the sub objectives were condensed in the light of new data from the case study. Identifying an informant and the key stakeholders in the case study setting helped in applying triangulation technique. Final interpretations were done in accordance with the theoretical basis of the research. This provided meaningful principles that have applicability in other settings too. An overview of the research design is provided below in table 3.1.

Table 3.1 An overview of the research design

Research Design	Description
Types of Research Questions	Phase 1: Questions about values regarding information security governance Phase 2: Questions regarding the usefulness of the proposed objectives from the previous phase.
Strategy	Two phase study: Value focused assessment through interviews and Case study
Data Collection method	Semi-structured interviews, case study, observations, secondary support documents in form of manuals and policies
Data Analysis	Phase 1: Value focused assessment steps as suggested by Keeney (1992) Phase 2: Data reduction, data display, triangulation
Theory Used	Value Theory
Major References	Keeney (1999), Catton (1954, 1959), Dhillon and Torkzadeh (2006)
Respondents	IT managers, IT Auditors, security professionals
Expected Results	Framework of means and fundamental objectives for maximizing ISG, principles of ISG
Validation Criteria	Klein and Myers' seven principles for interpretive field studies

3.5.3 Evaluation Criteria

The set of principles for evaluating interpretive research proposed by Klein and Myers' has been used to evaluate this study. The principles include the hermeneutic circle, contextualization, interaction between subjects and researcher, abstraction and generalization, dialogical reasoning, multiple interpretations, and suspicion. The fundamental principle of the hermeneutic circle refers to the idea of developing the complex whole from the meanings and the parts and their relationships. This signifies developing a complete picture about the context, the phenomenon and the complexities of the construct under study. The principle of contextualization requires reflection on the social and historical background to integrate the emergent situation in the field.

The principle of interaction between the researchers and the subjects shows the need for critical reflection on how the research data was socially constructed through the interaction between the subjects and the researcher. The principle of generalization deals with details that are revealed by the data interpretation through the application of principles one and two.

The last three principles point to the requirement of a degree of sensitivity on the part of the researcher to minute details of their data and findings. The principle of dialogical reasoning means that the researcher should be open to the idea that theoretical preconceptions might not be able to explain the case situations in the field. The principle of multiple interpretations alludes to the researcher showing sensitivity to the differences in interpretations of the participants to the same event. Lastly, the principle of suspicion refers to the sensitivity towards possible biases and distortions by the participants. These

principles were used to establish the validity of this study and a discussion on their usage is presented in chapter 7 of this dissertation.

3.6 Conclusion

This chapter established the importance of using individual values for development of ISG objectives. An outline of the philosophy, theory, methodology and the research design that is being followed in this study is provided. A discussion on generalizability of the results is presented. Based on the discussions in this chapter, an empirical investigation of ISG development and validation was conducted. Chapters 4 and 5 present the results of these investigations.

CHAPTER 4 Means and Fundamental Objectives for Information Systems Security Governance

4.1 Introduction

The purpose of this chapter is to present the means and fundamental objectives for information systems security governance. The objectives have been derived from the interview data gathered across 9 industries over a six month period. The chapter begins by providing a brief description of the profile of the respondents who were interviewed. This chapter then presents the list of means and fundamental objectives which emerged from the data. The discussion section presents the relevance of the proposed objectives in the light of research literature and establishes the contributions there of. The key lessons for practitioners of Information systems security governance are also listed. The concluding section discusses the results and establishes the need for the case study, which is subsequently presented in the following chapter.

4.2 Developing means and fundamental objectives

In the first phase of the study, a value focused approach is used to develop the means and fundamental objectives for information systems security governance. As discussed earlier, Keeney suggests a 3 step process to develop decision objectives from the values of the stakeholders in the decision context. Objectives in a multi objectives decision analysis model are generated in hierarchical fashion. The overall objective is defined first, followed by a definition of the fundamental objectives. These are the objectives that we actually wish to achieve in a decision context, as opposed to means objectives which merely provide a means to attaining our fundamental objectives (Kirkwood, 1997). A value

hierarchy helps in ensuring that fundamental objectives are appropriately related to the overall objective (Kirkwood, 1997).

In the context of this study, maximizing information security governance is the overall objective for the organizations in order to ensure an effective security program. The achievement of this strategic objective is affected by the various decisions that the people in the organization take. We seek to understand the fundamental objectives that apply to these decisions for multiple decision contexts within an organization.

4.2.1 Respondent profile

In an attempt to understand the values that affect ISG objectives in organizations, 52 interviews were conducted with a diverse group of individuals representing a broad cross section of industries and functionalities. The roles which the respondents were discharging included: Chief Executive Officers (CEO), Chief Information Officer (CIO), Information Technology Directors, Security Managers, Systems Administrators, Systems Auditors and helpdesk IT specialists. We also interviewed people with non IT job specializations for a generic and non-technical perspective about security controls. These respondents included managers and line staff workers from functionalities other than IT such as accounts, finance and human resources. The interview questionnaire template is attached in Appendix 1.

Participants in this study represent nine industries and represent a wide perspective on security governance issues. The industries included in this study are: Insurance, healthcare, credit card services, Banks, financial investment, energy, telecommunications, Internet service providers and real estate development, both in the private and government

sector. All the respondents had at least 5 years of professional work experience and significant experience of using IT. They are also under the purview of security governance practices. Some of the respondents do not directly work in information security governance domain but were included in the study nonetheless. We feel that the pervasive nature of security controls impacts everyone across the board in an organization and it is useful to get the values of even those people who were not directly responsible for developing and implementing these controls.

4.2.2 Keeney's three step methodology

Keeney's 3 step methodology is explained in this section to demonstrate how the steps were incorporated in the conduct of the first phase of the research. As Keeney (1999) suggests, the best way to understand the underlying values of people about an issue is to directly ask them. To understand the individual values, this study uses a three-step procedure as proposed by Keeney (1992).

Step 1: Listing Values

In the first step, Keeney suggests the development of a comprehensive list of personal values which might underlie the problem being explored. The process of identifying these values begins with interviews, which can be done individually or in groups. It is important to clarify the decision context of the study to the interviewees. Thus before the interview process, a guiding definition of information security governance was provided. We defined ISG as:

> Information Security Governance is defined as organizational structures, procedures and practices put in place to help in ensuring the integrity of the information flows and business continuity. Information Security Governance helps in protecting the information assets of the organization through the use of proper internal controls.

This definition provided clear boundaries for the scope of this research. The governance practices internal to the organization that affect the working of employees on a daily basis have been studied in this research. This research does not concern itself with the external practices such as relations with vendors or outsourced services.

We applied the process of listing the values which emerged during interview sessions with domain experts and other stakeholders in order to develop the objectives. The aim of the interview was to develop objectives for maximizing information security governance in an organization. The interviews continued with questions which sought to generate typical values and bring them forth for observation (Keeney, 1992) such as (1) probing for a wish list of the perfect characteristics for the ideal situation; (2) discussing the shortcomings of the proposed characteristics in real life cases; (3) considering actual work examples from the interviewee's experience; (4) discussing the consequences of bad decisions made; (5) asking the interviewee's about how others in the organization will be impacted by decisions and (6) generating scenarios to actually understand and cross check values being communicated.

People express their values in a variety of ways. In order to facilitate better understanding of what they meant, each respondent was interviewed individually and asked to explain their responses with examples. Probing further proved to be useful as the researchers developed a clearer perspective of exactly what a respondent meant. Thus, presenting

scenarios, interpreting consequences, understanding the constraints and goals of a decision context helped bring the values to the surface in a lucid manner. We extracted 260 values from the interview data and converted them into common forms (see Appendix b). After 40 interviews, we felt that the data had a lot of repetitions, which clearly pointed reaching a theoretical saturation in the process. Nonetheless, we conducted 12 more interviews to be exhaustive of all possible values about the decision context and reach a well informed theoretical saturation.

Step 2: Categorizing Values

All statements or the raw values for the problem context were changed into a common form. These common forms are subsequently converted into objectives. An objective has three features: a decision context, an object and a direction of preference (Keeney 1992). Decision context in this case is "What should the information security governance characteristics be in an organization?" Hence, each of the values that are listed by respondents is an object and the way to achieve this object becomes the objective. Thus the verb form of the object could be termed as the objective of that object. For example, data from the interview suggests a raw value such as ''Problems one comes across are usually lack of awareness about controls''. The value explicated above can be changed into a common form "Lack of awareness about controls is a problem", which in turn can be converted into an objective "Create awareness about control in employees". The decision context is related to controls, the object is awareness and the direction of preference is to have more awareness about controls. It is possible to derive more than one objective from a specific value statement, e.g. The maximization of education and training for security

governance is another objective that can be derived from the above value statement. As Keeney suggests, better alternatives for a decision problem can be generated once objectives have been established. This is opposite to alternative focused thinking where alternatives are first identified and then the objectives are specified. After striking down the repetitions in the data, we developed a list of 190 objectives (see appendix c).

Step 3: Relating Objectives

The list of objectives thus generated was arranged into clusters according to the underlying idea being conveyed by the objectives. After clustering, these objectives were rearranged through means-ends relationships (Keeney 1992). This basically involved classifying all the categories thus formed into either a "means" to the decision or an "end" to the decision objective for the problem context. Thus an objective that leads to another objective being considered in decision-making is a *means* objective whereas an objective which is fundamental and important in its own right, in the decision making process is called *fundamental* objective. This is primarily done through performing a *Why Is This Important* (WITI) test for each of the objectives (Keeney 1992). For example- 'ensure audit efficacy" objective does not directly impact information systems security governance in an organization. In its own context, the audit functionality gives an assessment of current state of controls and their strengths and weaknesses. It does so in a way that controls are developed and implemented in a better way, hence it is a means objective.

However, the objective "ensure continuous improvements in controls" directly impacts information security governance practices because if a security control is not implemented well, it creates vulnerability, thus weakening the governance process. Therefore "ensure

continuous improvements in controls" is a fundamental objective. Using similar logic, all the objectives are classified into either the means or fundamental category. Both fundamental and means objectives are important for the decision context. The set of fundamental objectives specify the core values which the decision should incorporate. The list of *means* objectives suggests areas of improvement for decisions based on the fundamental values. Our data suggests *six* fundamental and *seventeen* means objectives that are essential for information security governance in organizations. The next section presents a discussion on each objective and its relevance in achieving overall effective ISG in organizations.

4.3 Establishing the objectives in information security governance research

The fundamental and means objectives developed in this research need to be reviewed in the light of the existing information systems security governance literature. It is important to ground the developed objectives in extant literature to understand the implications of the objectives for research in this domain. Also, the grounding helps in interpreting the extent to which these objectives would be useful in establishing the information systems security governance agenda for organizations. The discussions about the fundamental and means objectives are presented in the two subsections below.

4.3.1 Fundamental Objectives

Establish Corporate Control Strategy (F1)

Our data suggests that developing a corporate wide control strategy is a fundamental objective for maximizing information security governance in organizations. It is important to define a strategic control plan that establishes the business requirements of information

systems security in order to make the organization achieve its business objectives. A control strategy maps the information security governance objectives to the business objectives and aligns the two. The strategic control plans should be then translated into operational controls that in turn set clear short term goals. As suggested by our data, it is crucial to develop a corporate security control strategy and ensure that security is a non-negotiable budget line item for the management. This involves developing a risks management strategy, understanding organizational power structures in developing controls and viewing security controls as cost of doing business. As observed by a senior IT manager in the electronics goods industry:

> Security control is a non–functional requirement and there is no place for non functional requirements in the system design. User groups do not talk about security, the so called non-functional technical requirement. How do you manage it? It becomes an issue of internal policies, and then it has to be related to IT architecture.

A control strategy ensures that security governance is an antecedent to complete security and process integrity. A control strategy requires developing guidelines using consensus and flexibility in tools for control. As mentioned by one of our respondents:

> "Security is addressed during normal strategic and operational planning cycles. Security has achievable, measurable objectives that directly align with our enterprise objectives. Determining how much security is enough is directly proportionate to how much risk and exposure an organization can tolerate".

Gregor et al. (2004) suggests a relationship between strategic planning practices and the value derived from IT. Business and IT management jointly create IT strategy, using the business strategy and objectives as the key reference (Peppard, 2001). Research in IT strategy stresses the need for top management to be closely involved in the IT strategy

process (Henderson and Venkatraman, 1993; Peppard and Ward, 1999), so that the IT strategy, upon implementation, results in IT systems that support the business strategy (Premkumar and King 1994). Consequently it is important to have a control strategy which ensures information security and thus helps in developing the IT strategy. Control strategy involves planning for the success of the security program. Having a centralized control strategy provides the departments with control plans that are required for successful implementation of security controls. IT strategy is a "macro competency" necessary for the success of IT (Peppard and Ward, 2004) and control strategy is important for the security of IT assets.

The use of inadequate control tools and inefficient internal practices for security has a negative effect on the management process and also compromises strategic objectives (Alves et al, 2006). Information security governance requires strategic direction and impetus. It requires commitment, resources and assignment of responsibility for information security management. It also requires a means for the board to determine that the intent has been met (Information Technology Governance Institute, 2006). Information systems control strategy is required to address information threats by conducting risk assessments aimed at identifying mitigation strategies and required controls (Da Veiga and Eloff, 2007). The control strategy should be an inherent part of an organization's IT strategy and overall business strategy in order to ensure that organizational objectives for both the short and long term are comprehensively met.

Encourage a Controls Conscious Culture (F2)

Culture creates and sustains connections among policies, processes, people, and performance (Julia and Westby, 2007). Our data suggests "establish control culture" as an important objective for information systems security governance. Developing control and risk consciousness in employees creates a "prevention mentality" that helps in minimizing intergroup rivalry over security initiatives. A control conscious culture interwoven into the fabric of the organization holds together all the technical, formalized and informal controls of the governance program. An environment where individuals "watch out" for each other strengthens the actual controls, leading to the achievement of the desired results. Also, with changing security needs, which in turn impact the controls, changes in the corporate culture too have to be formally taken care of. As a senior systems auditor from the healthcare industry commented:

> Changes being made in the corporate culture have to be managed in a better way. For instance, if the Internal Audit suddenly has to play a bigger role or a separate IS security department is required…all these things require a corresponding change in corporate culture. Why am I doing this? This needs to be explained better to people in MIS. If suddenly people are reviewing everything that you do…this kind of a change just has to be managed properly.

Management should establish ethical standards of conduct, which are essentially the rules to be followed by employees (Da Veiga and Eloff, 2007). Ethical considerations, such as maintaining employee's privacy, must be included by the management as a part of security governance program. The control consciousness is the general atmosphere in the organization, in which people perform their activities and carry out their control responsibilities. Controls must be implemented to protect the privacy of both the

employees and the customers. This enhances trust within the organization and with customers outside the organization (Da Veiga and Eloff, 2007). Communicating these measures is part of control awareness in an organization. All organizations have a set of unwritten norms and values to which their members subscribe. This cultural dimension is a powerful force in enhancing or compromising security (Dutta and McCrohan, 2002).

Maximize Clarity in Policies and Procedures (F3)

Security policies, procedures and guidelines are paramount in the implementation of information security governance as they provide direction and support (ISO 17799, 2005). Our data suggests that management should have clarity in security policies and procedures to make the implementation of the controls more effective and get the intended results from the governance process. Clarity in policies and procedures is essential to ensure the proper use of applications and technological solutions instituted in an organization. Controls should be reflected in the policy document and seen to be implemented through the procedures. As shared by the chief architect at a leading computer services organization:

> I think internal security controls are in the policy. In order to impose the policy, controls are developed, so controls in a way are policy. It helps you to ensure your policy.

Clarity in policies can be achieved through a structured approach to the development of user and operations procedure manuals, service requirements and training materials. Policies should be made easily accessible and reflect truly the control requirement in the policies. The high visibility of fair policies ensures that everyone follows the policy. Our data suggests that it is important to make the policies readily available for reference. It is

also vital to develop controls that follow procedures and are convenient to use. As mentioned by a senior auditor from a financial services industry:

> At the start, I just tell the auditee- if you just follow your security policies and try to implement the controls, you will be able to answer most of the questions, and there will be no problem.

There is a heavy emphasis on developing clear policies in information systems security governance (von Solms, 1996; Straub and Nance, 1990). Ward and Smith (2002) argue that the IT security policies also provide the basis for displaying the executive management's commitment to IT security. Moultan and Cole (2003) suggest that policies should be developed in a way that should facilitate the development of the relevant controls for security. In their proposed security governance framework, Moultan and Cole (2003) have identified "policies and procedures" as an objective. In their security governance framework, Eloff and Eloff (2005) place policies as a first priority for an effective governance program. In their proposed model, McCarthy and Campbell (2001) identify policies, procedures, documented guidelines and standards as crucial components for proper implementation of security controls. However, the policies should reflect the human, technical and procedural aspects of security management holistically.

Maximize Regulatory Compliance (F4)

Information systems security governance entails preparations for fulfilling the mandatory requirements of complying with relevant regulations. The governance structure should ensure compliance with external requirements as it is important for the organization to meet legal, regulatory and contractual obligations. Security governance practices are able to meet the regulatory requirements by identifying and analyzing external requirements for

their security impact and taking appropriate measures towards complying with these. Our data suggests that ensuring regulatory compliance is a fundamental objective to maximize information systems security governance. Regulations do not improve the governance measures efforts per se. To a certain extent, the regulations force an organization to rethink its security preparations and take actions which it should have taken anyways. As one of the respondents, internal auditor in credit card services industry, explained

> Five years ago our CEO did not know about controls, so we had to sit down and explain them to him. Over some time he was still in the process of getting it, but now he knows all about controls. It [SOX] helped a lot in increasing the popularity of controls. People are scared of SOX…we can just not fail and say I will do it next year. You have to keep testing till you pass. You have to be compliant.

Regulatory compliance has been a big driver in recent years to develop and shape security governance initiatives. As one of the respondents, Chief Executive Officer in a state agency commented:

> Regulatory compliance drives a lot of what we do. It also has an impact on your stock price. Control conciseness has come about in a big way because of this.

Compliance with regulation as a security governance objective has been extensively supported by literature (Da Veiga and Eloff, 2007; Tudor, 2000; Eloff and Eloff, 2005; von Solms, 2006; Moultan and Cole, 2003). Both internal as well as external compliance with policies and regulations requires preparedness and understanding of codes of practice, legal requirements and international standards. Dhillon and Torkzedeh (2006) classify compliance as a fundamental requirement for security initiatives.

Ensure Continuous Improvements in Controls (F5)

'Proper implementation of controls' has been identified as a fundamental objective for information systems security governance. Our data suggests that continuous and iterative control assessment helps in implementing the right controls in the correct fashion. Implementing controls requires caution to ensure minimum likelihood of disruption and errors in the functioning of the systems. Understanding the organizational context of particular controls helps in the implementation and adoption of controls. Our data suggests that to develop effective controls, implementation practices of an organization should use a "clean slate" approach i.e. start afresh and not superimpose old methods which will make existing biases impede the process.

Implementation of controls is not a one time phenomenon but an evolutionary exercise. It includes adapting the controls as per changing business needs. Managing the changes is crucial too, especially in a production environment. This requires analysis, implementation and follow-up of all changes requested and consequently made to the existing IT infrastructure. It is crucial that the changed roles reflect changed controls in the organization. As observed by a respondent, internal auditor in financial services industry:

> For example you make a great access control upfront and don't come back and look at it again. So we could point out some of those issues. We try to make sure that you develop something, to take care of those processes where it has holes. So if somebody changes roles, changes jobs or the organization restructures, what controls do you have in place which ensure that you change your procedure accordingly? Or then you have to consider- do the procedures need to be changed? So there is a lot you have to think about.

In his security management model, Booker (2006) identifies "implementing a holistic approach" as one of the objectives for good security governance. The author suggests that all the security requirements of the organization should be exactly mapped to the controls

and implemented precisely to provide a holistic security governance approach. Realizing the importance of the control implementation process, ITGI has a domain of activities and objectives dedicated to successful implementation of controls in its governance framework, COBIT (2007). In the *Acquire and implement* domain of COBIT, seven objectives are identified. All these objectives suggest a meticulous implementation process. COBIT even emphasizes the importance of managing changes [objective AI6 (Manage Changes) of COBIT] for successful ongoing implementation, which is similar to what our data suggests. COSO framework, in its *control activities* component describes the impact of well implemented relevant controls on security environment of the organization. Eloff and Eloff (2005) argue for proper execution of security controls to develop a secure IT infrastructure and to maintain the control environment. Rees et al. (2003) identify the importance of proper controls implementation in their security governance model.

Enable Responsibility and Accountability in Roles (F6)

Our data suggests that responsibility and accountability in structures is essential for good information systems security governance. Clarity in roles and ownership of decisions in the organization helps in aligning security governance goals with business goals. Some of the sub-objectives associated with this objective are 'discourage sudden changes in responsibility structures', 'define and document roles and privileges properly' and 'encourage transparency about accountability for actions'. The groups of sub-objectives argue for a stable, well-defined and clearly communicated responsibility structure to provide right direction to the security practices. Clear role differentiation encourages

accountability of the managers and results in better alignment of personal motivations of the individuals with organizational expectations. As one of our respondents commented:

> Roles and responsibilities have to be very clear upfront. Nobody should be surprised at their work by having to do something which they were not doing yesterday. Making sure that people understand the priority, roles, responsibility is important. If you can demonstrate this, then you can get the level of service required.

In a global survey of IT managers regarding 'what activities should be a part of information systems security governance', about 94% of the respondents emphasized alignment of roles and responsibilities and accountability as a crucial activity (Deloitte, 2006). Thus it is important to encourage ownership of data sources and assign appropriate roles and privileges to managers in order to carry out the governance objectives effectively. It is also true that organizations can allocate roles and authority but responsibility can only exist once it is accepted (Drummond, 2003). Accountability, thus results when the responsibility is accepted by all parties to ensure that all the resources are used for authorized uses and such actions can be traced back to the responsible person (GISP security principles). Hence it is absolutely essential to communicate the importance of the roles to the managers.

To summarize, the list of six fundamental objectives for information security governance is presented in the table 4.1 below. Under each objective, the corresponding sub objectives are shown.

Table 4.1 Fundamental objectives for information security governance

	Objective Name	Sub-objectives
F1	Ensure corporate controls strategy	Develop corporate security control strategy Establish a risk management strategy Ensure that security governance is a non-negotiable budget line item Understand organizational power structures while developing controls View security governance as a cost of doing business Ensure that security governance is an antecedent to security and process integrity Develop guidelines using consensus Develop measurable security control objectives Ensure departments have control plans Develop flexibility in tools for controls
F2	Encourage a controls-conscious culture	Establish a control- consciousness culture Develop risk consciousness in the employees Establish a security conscious culture Create prevention mentality Encourage appreciation for security governance culture Establish a culture where individuals watch out for each other Encourage an environment of conformity Instill the desire into the employees to meet expectations about controls
F3	Maximize Clarity in Policies and Procedures	Enhance visibility about fairness of policies and procedures Create controls which logically follow the procedures Create convenient policy Define control policies for access to information resources Ensure compliance with policy document Ensure policies are readily available Reflect control requirements in security policies Encourage discussion on internal controls as identified in the policies
F4	Maximize Regulatory Compliance	Define controls for compliance with regulations Encourage regulatory compliance through internal controls Encourage respect for laws of the society Ensure that compliance is a substantive and sustained improvement in business processes Establish a compliance culture Explain the importance and need for compliance to technical people Follow regulations in entirety Formalize process of compliance in the organization Understand the impact of regulations on controls Use regulations as a catalyst for implementing better practices Avoid turning compliance into “check the box exercises”
F5	Ensure continuous improvements in controls	Ensure continuously iterative control assessment and implementation Maintain and integrate the controls properly in changing business needs Change controls with process changes Effectively test the controls Manage changes efficiently Manage changes in production systems Manage controls from the source of problems i.e. employees Understand the organizational context of controls implementation

		Use clean slate approach for controls implementation Develop effective change management practices
F6	Enable responsibility and accountability in roles	Create organizational responsibilities for compliance Define responsibility and accountability of controls for security governance Discourage sudden changes in responsibility structures Encourage a sense of responsibility Encourage individual responsibility for ensuring proper access to data resources Encourage responsibility sharing Ensure accountability Assign responsibility for protecting information Define and document roles and privileges properly Encourage transparency and accountability for actions Encourage individual responsibility for ensuring proper access to data resources Ensure responsibility and accountability sharing in protecting information Ensure job design around IS needs

4.3.2 Means Objectives

Ensure Efficacy of Audit Processes (M1)

Efficacy of auditing, on the part of both the internal and external auditors, is essential for assessing the progress of the organization on various security governance fronts and the efficiency of the efforts in this direction. In this research, "ensure efficacy of audit processes" has emerged as an important means objective which essentially inserts checks and balances into the governance program. Audit practices are essential for ensuring that the management is incorporating adequate consideration towards the changing context of governance tasks. Our data suggests that internal auditors can be treated as consultants to ensure effectiveness of the controls. Talking about the role of auditors in internal control assessment, the chief audit officer of a fortune 500 organization in credit card services industry mentioned:

> We do not create controls, we only test them. We consult about them and we tell them [auditee] here is the type of control you will need to have and you will have to create it because that's your job. If you need help in creating those controls, we can provide some guide lines and come back and see how well you have done it.

It is important to provide adequate access to the auditors across the organization and establish a cross checking mechanism for the audit function. Auditing helps in integrating the information rules into daily management practices. Periodic internal audits with well defined objectives and scope can help in enhancing the security governance mechanisms in an organization.

Auditing is an important functionality which provides assurance for risk management, controls and governance structures (Institute of Internal Auditors, 2006). Organizations may regard strategy, people, assets and finance as pivotal but equally so are routine day-to-day aspects of an organization including the mechanics of the IT system. Thus auditing becomes crucial to provide a reasonable assessment of risks of day-to day jobs in IT and suggest improvements for better security of information systems. It is vital for management to consult experts proactively and to advise on IT security (Trcek, 2003). Auditing ensures segregation of duties and points out anomalies in normal business transactions. Lack of segregation of roles and auditing of the suspense account were the major cause of the failure of Barings Bank (Drummond, 2003). This is ssentially an example of security governance loopholes. Internal auditors are responsible for pointing out management deficiencies negatively impacting the strength of an organization's internal control (Banks, 2004). The greatest benefit of audit function is its unbiased assessment of management adequacy. A strong, independent audit committee can be critically useful in ensuring high quality of reporting and controls and the proper identification and management of risk (Wagner, 2000).

Maximize Clarity in Business Processes (M2)

Our data suggests that it is absolutely essential to maintain the integrity of business processes for proper security management. To maintain the integrity, it is essential that there be clarity in how these processes work, so that proper controls can be instituted in the right places. Business processes need to be clearly understood and awareness of normal business activities should be increased. As explained by an internal auditor from the financial sector:

> The application should not be a black box. We should understand the business processes. What is it that it is doing? How does it convert the input into output? Whether the whole processing it is doing is correct or not, should be clear.

If the implemented controls make it difficult for the people to perform their day-to-day job efficiently, there is a greater possibility of these controls being circumvented. As observed by one of our respondents:

> The practices do not take into consideration the impact on the user's performance. The introduction of new requirements in an existing process necessitates additional effort on the part of the user. This effort is often perceived negatively because it can be intrusive, complicated, unclear, or draining.

Business processes can be described as "a set of ordered activities, controlled by central vision which consume resources and use information". Adequate information security governance has clearly defined business processes (Alves et al, 2006). Efficiently designed processes reach maturity faster, hence can be protected better. It is important to recognize that security requires an end-to-end view of business processes (Dutta and McCrohan, 2002). A clear and holistic view of business processes can lead to a comprehensive security governance program. Moulton and Coles (2003) argue that implementing and

ensuring effectiveness of governance requires business process information risk management (BPRIM) approach. This approach recommends that business process owner must appreciate that risks arise due to faulty business processes and the information that they use. It is imperative that the management inserts and enforces controls related to the risks throughout the business process. Along similar lines, Banks (2004) argues that organizations should not change job descriptions, employees or business practices without first examining the impact of these changes on controls. A sudden change in business process can create vulnerability from the security management perspective and should be avoided.

Ensure Communication about Controls (M3)

Our data emphasizes the significance of sound communication about the controls. It is important to clearly communicate the various consequences of non compliance with controls, the nature and scope of the controls themselves and consequences of possible control breaches that can occur.. Our data also suggests that organizations should encourage communication about control issues amongst employees. It would be helpful to have a communication policy that results in frequent internal debates about controls in the organization. Employees would be better prepared to follow the controls if they are aware about the rationale, purpose, risks and values of the controls and the reasons governing organizational actions. Communications acts as the backbone for a successful security governance program. As one of the respondents shared about his organization:

> Communication, discussion, and debate on controls topics are encouraged. Such exchanges are conducted in visible, open, participative forums, both formal and

> informal, as appropriate. The security actions and their contribution to mitigation of enterprise risk are well known throughout the organization.

The failure to regularly and effectively communicate information security policy, standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and the consequences of failing to comply to all relevant parties can cause unintentional breach of policy by parties to whom the policy has not been effectively communicated (GISP, 2006). Such failure can also result in the intentional breach of policy by parties to whom the adverse consequences of such a breach have not been effectively communicated. COBIT 4.1 (2007) emphasizes the importance of constructive communication between IT and other functions within and outside the business for security governance. COBIT identifies, *communicate management aim and direction* (PO6), as an important objective that stresses the importance of ongoing communications policy to articulate the vision and the objectives of security governance program. In COSO framework, information and communications, the capture and communication of relevant information for integrity of controls is proposed as an objective. Leach (2003) observes that it is important to gather input from staff on the precise points where the body of available information is being undermined by confusing messages in the company's pronouncements or contradictory practices in its systems. Open communications help employees' form a clear picture of the intent and scope of the controls.

Ensure Alignment of Individual and Organizational Values (M4)

Our data suggests that it is very important for the individuals in an organization to be able to identify with the organizational goals. "Ensure alignment with individual and

organizational goals" has emerged as a fundamental objective in this research. It is important for the management not to contradict the values being imposed on employees by setting conflicting managerial and security goals (Ruighaver et al, 2007). There is a significant cost to be paid for not understanding individual values about security governance and not attempting to reconcile these values with those of the organization at large. For the proper alignment between individual and management security goals, values of people about security governance should be reflected in the objectives developed by the management. As observed by the chief security officer of a state agency:

> Information security should flow from bottom-up; people with their hands in the actual work should influence information security governance policies with guidance from the top.

This objective articulates the need for understanding an individual's attitudes and beliefs about security and how their behavior is influenced by peers. It is important to promote certain values in individuals for better security governance. Some of these values, as suggested by the interviews, are: respect for others, privacy, integrity, self-pride in job and honesty. As observed by one of our respondents, a compliance officer in insurance industry:

> Personal integrity influences information security governance practices a lot. No matter what laws are in place, if your own values are not upright, there is little that would stop you from behaving unethically.

The importance of individual values for better security governance is also established in the literature. Leach (2003) argues that an individual's personal values and standards of conduct is a major determinant of the willingness of that person to stay with the organization and conform to the established norms. Most people ascribe a high importance

to shared values and sensible rules. Such employees are also expected to imbibe and apply the organization's value system and standards of work to their own preconceived and individually accepted set of rules. If there is a conflict between an individual's values and organizational values, tension arises and most people are unable to sustain in such an environment for long (Leach, 2003). As one of our respondents, an HR manager at a state agency mentioned:

> It is important to acertain whether one's personal values/norms are the same as the company's or not. If they are not, then most likely his behavior would negatively affect the security governance.

Values provide keys to reach an understanding on how people evaluate the organization and its measures for governance (Jones and George, 1998). If the values embedded in the security measures do not match individual's values, chances of the failure of such measures increase drastically (Baskerville and Siponen, 2002; Warman, 1992; Angell, 1996). It is important to involve end-users in control development process so that too complex and stringent controls do not result.

Ensure Data Criticality (M5)

Information systems security governance measures must protect the integrity of critical business data. This requires acquiring and maintaining technology infrastructure that satisfies the business requirement of providing the appropriate platforms for supporting business applications. It is important to maintain the integrity of the electronic data for the accuracy of business decisions and for meeting regulatory compliance criteria. An IT governance manager from a state agency in California suggests:

> Security governance safeguards information against unauthorized use, disclosure or modification, damage or loss by implementing logical access controls. These controls ensure that access to systems, data and programs is restricted to authorized users.

Some of measures to establish criticality of the data, which our data suggests, are through assessment and classification of data. The various parameters governing this are sensitivity, identification of data owners, assigning of responsibilities according to information criticality and linkages of data with authorizations. Articulating the need for protected data, one of our respondents says:

> With data resource, you have to specify data ownership. Some body needs to own it and resources should be classified, according to their sensitivity, whether it is proprietary information or not. Access to those data resources should be restricted except by authorization which should come only from the data owner. It should be granted on roles. Access should be given to roles rather than individuals.

It is imperative to ensure that data remains complete, accurate and valid during its input, updation and storage. It is also important to establish data integrity for compliance purposes. Data integrity and auditibility of data resources is a big part of compliance efforts (Volino, 2004). Establishing data criticality through confidentiality, integrity and availability has been enthusiastically supported by security governance researchers (Finne, 1996; Sherwood, 1996; Ward and Smith, 2002). ISO/IEC 27002 identifies *asset classification and control* as governance objective for information systems security. Access control and authentication rules (Sandhu and Samarati, 1994) have been considered very significant for proper governance structure. Booker (2006) argues for maintenance of a database critical network and information assets for better security governance. A secure

and reliable IT infrastructure can only be created though the institution of proper protection mechanisms for critical data in an organization.

Ensure Punitive Structures (M6)

It is important to establish deterrence criteria to communicate the consequences of non compliance with controls and policies. Our data suggests that it is of paramount importance to ensure disciplinary action in case of unethical behavior or against law breakers. Establishing clear consequences for not complying with controls and explaining the disciplinary actions signifies the seriousness and commitment of the management in instituting the controls. It is also important to explain the meanings of criminal actions to the employees. A respondent said:

> You have to make the consequences of the action very clear. Most of the times, companies do not make it clear. They warn them saying "if you do that, criminal action will be taken". But what is the criminal action? People are held responsible for breaches, but it's not clear that if breaches happens, what action would be taken?

Deterrence criteria help in creating the fear of punishment amongst employees which in turn cultivates conformity with rules and regulations. Developing countermeasures to deal with destructive actions is required in order to ensure quick and effective responses in case of security breaches. One of our respondents added:

> Some of the governance practices may not work because the people involved have personal agendas such as wanting to meet deadlines even if it means not adhering to company policy. People will continue to put the company in financial and operational risks until they experience the consequences for doing so.

Deterrence criteria for security have been emphasized in information systems security research. Dhillon and Torkzadeh (2006) argue for developing deterrence criteria for better

security. Straub (1990) and Straub and Nance (1990) have used the general deterrence theory from criminology, which suggests sanctions to prevent people from committing crimes. The theory suggests that it is prudent to maximize prevention and deterrence and thus minimize abuse. There has not been much work about deterrence criteria in security governance research. Most of the leading standards for security governance such as COBIT or ISO 27000 do not mention deterrence as an objective. Research models in security governance also do not emphasize deterrence activities as an important objective for governance. However, our data suggests that deterrence is an important objective when controls are used as a governance mechanism.

Ensure Clarity in Control Development Process (M7)

Our data suggests that establishing clear control development process creates transparency in governance efforts and creates a favorable perception of the controls in the organization. It is important to create systemization in control development process and define achievable objectives. Critical data or business processes should be protected by multiple layers of controls, so that in the event of one set of controls failing, there would be other sets of controls to fall back upon. The chief architect of one of the leading IT services firm in the USA observed:

> For example, we made sure there no single point if failure, by providing layers of protection through logins. Unfortunately you have to remember more than one password for this. Particularly vexing is that anything different from your daily desktop login, and you have lot of problems remembering it. But everything can not be convenient, and people are getting used to it as there is no other option.

Change initiatives also require development of fresh set of controls at all levels. Controls should be simple, flexible, timely and easy to use. Security controls could be developed by

structuring information needs and performing risk assessment to understand the scope of their impact. There has to be a balance between stringent and usable controls for the security governance environment to prosper. The Chief Information Officer of a leading insurance firm commented:

> Yes, we want to create environment of innovation and creativity. People are free to do what they want to do but I would say within the framework. So we define the framework within which people can freely move but retain enough controls so that people do what they have to do

COBIT (2007) touches upon the development of application level controls and emphasizes clarity in the process. NIST, in its special publication (800-53 revision 2, 2006) provides guidelines for selecting and specifying controls, specifically for information systems supporting the agencies with federal government. The guidelines suggest creating a foundation for the development and assessment of security controls determining the governance efficiency. COSO, in its controls activities phase, touches upon the process of defining security objectives. It calls for transparency in the process for better fits with the organization. There is a lack of discourse in research literature about the process of development of security governance objectives and the actual controls which follow from this process. Definitely, there has not been much guidance on how to develop effective controls. This research suggests establishment of clear control development processes.

Ensure Formal Control Assessment Functionality (M8)

Establishing "formal controls assessment" functionality has emerged as a "business requirement" for successfully governing information systems security. Our data suggests that the controls assessment functionality enables continual assessment and improvement

of controls. A formal entity for control assessment ensures that appropriate controls are designed around information systems needs, where company's assets are protected, bureaucratic delays are avoided and stakeholder viewpoints are reflected in the governance process. As suggested by a database administrator in a state agency:

> It is very difficult to take into account how each employee conducts their job responsibilities and design IS around that, but ideally each employee job function and needs should be looked at and incorporated in the IS design

It is important to differentiate between lines of business and industries before applying popular controls which are being used by others. A periodic cost benefit analysis and IT architecture review for the appropriateness of a particular design for the security controls should be performed by such an entity. The Chief Information Officer from a state agency explained:

> In controls assessment for internal system, we perform what we call security architecture review. Anything that goes into the production is part of overarching set of policies. Look at our governance model, one dimension is change control. Part of our change management process is security architecture review for application developers, purchasing officials, to check if this meets security guidelines.

Instituting formal control assessment functionality also discourages implementing controls as an "afterthought". It is important to understand how and why controls work and what can be done to make them more effective. This can be the chief responsibility of such a business unit. As mentioned by a senior auditor at a state agency:

> You go though it [control] and make sure it is ok and put it in production. This is what I had done to improve it, so we try to check a lot of those or test the procedures. We try to make sure, do you have it? Or the segregation of duties? Which is the set of developers who approve the actual production? We take a lot of their input because it's crucial for the controls, so they know exactly how it has been done.

Establishing controls assessment as functionality helps in managing the IT investment for security. Control assessment as a functionality meets the need of the business requirement for funding and controlling disbursement of financial resources. Security governance would be more effective if there are regular investments made in this area and an operational security budget is established and approved by the organization. Our data suggests that a formal entity for control assessment could help in achieving several sub objectives for security governance. Some of these are: explaining prioritization of tasks and actions for organizational members, establishing the relation between controls and IT architecture, ensuring good IT architecture, developing dynamic controls structure and balancing centralization vs. decentralization and effectiveness vs. usability.

The existing frameworks of information systems security governance do not have a clearly articulated objective of this kind. But there have been discussions on the various functions that the control functionality would perform. For example, security investment, a sub objective for control assessment functionality, has been researched arduously over the years. It is difficult to make security investment decisions as it requires calculation of net benefits expected from the investment (Ryana and Ryanb, 2006). Calculation of net benefits from security is difficult but required nonetheless. As Dhillon and Moores (2001) suggest, key to controls implementation is to identify the exact level of resources allocation needed. The amount spent should be proportional to how critical the data is, the cost of controls and probability of the occurrence of the event. Ryana and Ryanb (2006)

argue that investment in security initiatives results in greater freedom from successful attacks and the system survives longer before actually succumbing to such an attack. The role of IT architecture in managing security is also acknowledged by research literature. Dynamic business environment and sophisticated security needs call for newly formulated IT architecture demands and revised assumptions about design and deployment of information systems (Melling, 1994). Such architectural shifts have strategic implications for the organization. Amer and Hamilton (2008) claim that it is important to have a security architecture which governs and ensures that various security related tasks are deployed correctly. Appropriate controls need to be designed along the way inherently in the business process as the IT infrastructure of an organisation evolves. Organization make important business decisions on real time information but there are hardly any assurance methods associated with data of this kind (Flowerday and von Solms, 2005). Current auditing practices provide assurance months later which might be too late. Appropriate and timely controls to mitigate such risks are required and the oversight from a formal body are playing increasingly important roles in the integrity of such data. It should be capable of arranging for continuous auditing on demand (Flowerday and von Solms, 2005). Hence we infer that some of the points that we have emphasized under this objective, have been touched upon in literature but there is no direct call for establishing controls assessment as a separate functionality. Our data suggests that this is something which needs to be done.

Maximize Monitoring and Feedback Channels (M9)

Our data suggests that security governance requires effective and established channels for monitoring the controls and incorporating feedback for further enhancements. Monitoring the controls helps in achieving the performance standards set for IT processes. Establishing monitoring and feedback channels as a security governance objective requires commitment to continuous reviewing, getting feedback from people and assuring that "what is being claimed" is done. As shared by the Chief Information Officer at a state agency in Virginia:

> Nothing can derail a security initiative and change management quicker than agitating employees. Whether it is a VP or a CFO, if people feel you are not being responsible and are taking control away from people or trying to impose it, it makes people jump through hoops.

Periodic review from external auditors helps in providing a fresh perspective about the controls. Review and feedback about the controls should be encouraged on a daily basis. Our data suggests that it is important to review the controls with respect to the organizational objectives and analyze the existing gaps. As explained by chief architect at a software service provider organization:

> There are certain controls which are not liked by people…more pertinently, people hate them! How you go about making sure that controls are effective? Well! We do have some feedback processes wherein people register their concerns. After all internal control is the most important part of security.

Monitoring of employee behavior includes monitoring the installation of unauthorized software, use of string passwords and keeping records of internet sites visited (Da Veiga and Eloff, 2007). Technology monitoring could include installation of sniffers for incoming and outgoing data packets, capacity and network monitoring. In COBIT (2007), there are four domains for managing information technology and monitoring and evaluating one of the domain in this model. In this domain, all IT processes need to be

regularly assessed over time to check their compliance with controls (ITGI, 2007). This domain prepares the management to ask difficult questions such as; 'How well is the organization prepared to assess the effectiveness of security controls?' 'Can IT performance be linked to business goals?' (ITGI, 2007). COSO (2006) too emphasizes on monitoring to ensure that controls give the intended results. Internal auditing can help in the monitoring process as well. Monitoring the effectiveness of controls is a difficult and ongoing process (Dhillon and Mishra, 2006). There is no mention of feedback channel in COSO though. Tudor (2000) defines "monitoring compliance" as a security governance objective which is critical for protecting IT infrastructure. Rees et al. (2003) emphasize that all control processes should be monitored and reviewed. In their proposed model, feedback is considered critical to a successful governance program. Every stage of the model suggested is followed by a feedback channel so that there is continuous improvement in the process of governing security. Kolokotronis et al (2002), in a proposed multidimensional multilayered security governance model, suggest monitoring as a crucial objective for managing security controls. The authors also argue that monitoring of the controls should be done at a corporate level

Ensure Visible Executive Leadership (M10)

Visible leadership for security governance entails a philosophy and style which promotes security controls throughout the organization. Our data suggests that establishing executive leadership in visible roles fundamentally helps in improving the perception of security governance in an organization. As suggested by our respondents, executive leadership should be able to "walk the talk" and should lead by example. Such behavior generates

respect for the security leaders and encourages key individuals to enforce rules and remedial solutions effectively. As one of our respondents collaborated;

> There has to be strong leadership, reinforcement of a tie between what's being done and its value and risks. Also practice what you preach. It helps to have IT personnel in visible positions with good commitment being shown from top executives.

For a strong foundation for information systems security governance program, it is important for the leadership to nurture relationships with the employees. As our data suggests, in order to promote the security governance initiatives, it is important to put committed IT personnel in visible positions and encourage a control conscious attitude on the part of the supervisors. Having an enthusiastic manager to lead the security governance initiatives goes a long way in shaping the perception of the people about security. As one of our respondents, a manager in accounting department of the insurance industry explained:

> Leaders should understand their accountability and responsibility with respect to security for the organization, for their stakeholders, and for the communities they serve, including the Internet community and the protection of critical national infrastructures.

Research literature in information systems security governance argues for a strong leadership for the success of security governance program. Committed leadership is required to manage resources for the security program. It is necessary that senior leaders should be seen to be visibly engaged in the management of enterprise security program and champion the security cause (Julia and Westby, 2007). Also, senior executives should accept the responsibility of the success of their security programs. Security leadership should be responsible the sponsorship, strategy and return on investments metrics

(McCarthy and Campbell, 2001). Tudor (2000) emphasizes the importance of executive sponsorship in developing security infrastructure for better governance. Leadership in terms of guidance and executive level presentations is a key objective for security governance (Eloff and Eloff, 2005; ISO 17799, 2005). Da Veiga and Eloff (2007) propose leadership and governance as a primary objective for a comprehensive security management program both at strategic and operational levels.

Maximize Group Cohesiveness (M11)

Group cohesiveness, as a security governance objective, informally creates a favorable environment for the actual use of the security controls. As the data suggests, group behavior can greatly influence and shape individual perception about security controls. Norms of security behavior influences cohesive groups better and more profoundly than groups with disagreements. As mentioned by a help desk staff at a state agency:

> I think the biggest influence to individual and group behavior towards IS governance is peer pressure. On always look around to see if everyone else is following or not following the controls.

Also, with cohesive groups, an individual gets few opportunities of feeling left out and be disgruntled. Our data suggests that it is important to have cohesive groups which perceive security governance initiatives positively. Enhancing group cohesiveness can be achieved through acquiring and maintaining a motivated and competent workforce, thus maximizing personnel contributions to security. Acknowledging the impact of peer pressure in group behavior, security governance should comprise of active measures to enhance team spirit through sound personnel management practices.

Managers should pro actively initiate measures to enhance group cohesiveness. As our data suggests, some of these measures could be: encouraging the tendency to share the work and credit for good work, respecting personal integrity and values, restricting personal competition within the group, discouraging favoritism and self interest in groups and understanding when the group's behavior changes due to peer pressure. Even though an objective such as "enhance group cohesiveness" does not give tangible benefits in the short run, it is nonetheless essential for the well being of the security governance measures in the long term. Director of Integrated Systems Security department at a state agency observed:

> A person's ability to give credit where credit is due; appreciation to others for their work, not taking undue individual credit for group work is important for the group to work together.

In information systems research, the importance of group solidarity has not been emphasized specifically for security or governance related works. Eloff and Eloff (2005), in their security governance model, describe "developing teams" as an objective for governance. This component describes employee's responsibilities towards security and aims at creating an improved control culture. But organizational behavior and social psychology research have long argued for encouraging the formation of cohesive groups within organizations (Lepine and Dyne, 2001) for meeting business objectives. It is important to have teams and groups that can carry out governance responsibilities to meet security objectives. Well planned security initiatives need even better planned execution by responsible members. Much of the work in organization is completed through teams. Success of a team is a function of team member's talents and available resources, but also depends on how such team members interact to get the work done (Marks et al., 2001).

People derive part of their identity and sense of self from the work groups to which they belong (Hogg and Terry, 2000). This is significant in terms of security management, as even minor deviations from the expected role could be catastrophic. From security governance perspective, it is important to understand how group membership based self definition produces behavior which is in sync with the group (Hogg and Terry, 2000). Such strongly motivated security groups can shape security perception and behavior and influence the culture of the organization positively for better security management. After all, organizations rely on employee initiatives in order to perform effectively (Hogg and Terry, 2000) and security governance is no exception.

Maximize Management Commitment (M12)

Our data suggests that "maximize management commitment" objective for security governance initiatives can actually decide the fate of the controls instituted. Management needs to actively participate in the entire control development-implementation-monitoring process from end to end in order to establish effective controls as a "top priority". As mentioned by a senior auditor from the health insurance sector;

> Security governance needs to be driven from the very top of the organization to down. Unless it's starts at the top, it is difficult to enforce it at a lower level. They [management] set the tone for the entire organization. If the people know that the executives are continually violating the policies, they will think that policy is not important. Executives should be self aware in the compliance era, since they are the driving force behind the security initiatives.

Managing security governance efforts requires setting of priorities for resources invested in controls. Also, management needs to reward conformity with controls, develop an environment that facilitates control adoption, provide recognition for good control

behavior, instill good values about controls and ensure that it is accessible at all times. As observed by information security manager in an educational institute:

> There should be positive reinforcement for doing the right thing and doing things right; and there should be negative consequences for failure to do so.

It is wise to assess the damage to the organization and to individuals from lack of the controls. Management should proactively encourage values such as dedication, determination, open mindedness and truthfulness for a secure environment. Providing appropriate attention to all stakeholders in the organization and instilling the desire to meet the expectations from the controls is important for long term success of the governance program. As a respondent from internal audit division at a Bank said:

> With respect to oversight, planning, and performance, security is treated in the same fashion as any other business requirement. Security is considered a cost of doing business, not a discretionary or negotiable budget-line item that needs to be regularly defended. Business units and staff don't get to decide unilaterally how much security they want. Adequate and sustained funding and allocation of security resources are required as part of the operational projects and processes they support.

Research literature in information systems security governance calls for greater management participation for the success of security initiatives. Moultan and Cole (2003), in their security governance model, identify "management's role" objective as an important dimension for the success of the security program. Management should foster a control environment that encourages high level of integrity and professional standards. The involvement of the senior management with security agenda is a key to achieving good security governance (Ezingeard, McFadzean and Birchall, 2005; ISO 17799, 2000). Information security can only be established if senior managers give it their complete

support and commitment (Von Solms, 2001). It is the management's responsibility to convey it's seriousness about governing security matters and emphasize the strategic benefit of the controls implemented. It is difficult to implement the appropriate plans for security strategy with the support of the top management (Kankanhalli *et al*, 2003). McCarthy and Campbell (2001) emphasize the importance of security and user management for better security governance and propose a crucial role for the management to ensure success.

Maximize Resource Allocation for Controls (M13)

In this research, "maximize resource allocation for controls" has emerged as a means objective to maximize information systems security governance. Management needs to do a lot of groundwork before developing the actual controls for security. This objective suggests that organizations should take some proactive initiatives in order to develop conducive environments for effective control development, implementation and monitoring. Our data suggests initiatives such as allocation of resources, coordination of multidisciplinary functions, enhancement of measures like trust, development of an environment for free and politics-free environment, as being a precursor in resources allocation. These control initiatives act as an antecedent to creating a control friendly environment and aligning the business strategy with the security strategy of the organization.

Security is often treated as the job of IT people and controls as part of accounting department domain. Resultantly, there could be potential conflict or lack of responsibility

between the two departments resulting in compromised systems. These tensions need to be resolved. As suggested by a senior auditor, retail industry:

> Plug the gap. MIS and Accounting have to play in the same sandbox. Both departments have to understand that they are trying to resolve the same issues of securing information.

An environment of politics and fear can undermine the seriousness of security controls. It is therefore important to create fear-free conditions where individuals can voice opinions about use and relevance of controls. One of our respondents adds:

> Secrecy creates fear, which ultimately leads to someone making a mistake by letting information out. Caution would be a better value to push because it allows for openness, but not fear to occur.

Research literature on information systems security governance does acknowledge the importance of some of the proactive initiatives as suggested by our data, but does not accord the same importance to all. According to von Solms (2000), trust is the most important issue in establishing information security governance in an IT environment. The fundamental question that needs to be asked is: 'Can I trust the entities I depend upon?'(DeMaio, 2002). Management and employees should have mutual trust for each other for implementation of controls and procedures and also to guide employees through changes in security behavior. Often good security plans fail due to lack of proper resources and guidance. It is critical for the management to ensure that adequate resources are allocated to support the overall enterprise information security strategy (Information Technology Governance Institute, 2006). For getting enough resources, the security department needs to make a good business case for security. As observed by a project manager, electronics industry:

> Security is a non–functional requirement. There is no place for non functional requirements in system design. User groups do not talk about security, as this a so called non-functional technical requirement. How do you manage it then? It becomes an issue of internal policies.

One of the obstacles in engaging senior executives to address information security is the difficulty of connecting security expenditures to profitability (Dutta and McCrohan, 2002). It is imperative that the business value of security expenditure be justified to the management. Our research indicates that expenditures in security are intricately linked to business continuity and hence the very existence of an enterprise. In the review of literature, we did not find an explicit support for many of the security initiatives as suggested by our data. We believe that this is an important finding and has the potential to dramatically change the success of governance efforts.

Encourage Standardization of Controls (M14)

Our data suggests that "Standardization of controls" as a security governance objective helps in improving and assessing the nature and impact of security controls against the mechanisms employed by other players in the industry. This provides avenues for improvement by learning from others. Benchmarking security investments and governance practices with industry standards provides motivations for improvement and implementing innovations in the existing control practices. As voiced by an internal auditor from the energy industry:

> An organization should regularly compare and benchmark its security state, investments, and actions with others in its market sector and community of practice.

It is prudent to compare the state of controls with standards across the industry and, in the process, standardize the control development process within the organization. Our data suggests that it is helpful to refer to the prevalent industry models and frameworks for control formulation as it provides a baseline to start with. As a project manager from a Bank responded:

> Security is integrated into enterprise functions and processes. These include risk management, human resources (hiring, firing), audit/compliance, disaster recovery, business continuity, asset management, change control, and IT operations. Security is actively considered as part of new project initiation and ongoing project management and during all phases of any system-development life cycle (applications and operations). Security controls should be standardized to be able to fit into the other processes seamlessly.

Research literature in security governance is in favor of standardizing the controls. Standardization is a process of alignment and entails stabilization and closure in definition and boundaries of the standard (Hanseth et al., 2006). Some of the potential benefits of standardization are that management's performance can be judged by how well the organization performs in terms of internationally accepted information systems security governance practices. (Eloff and von Solms, 2000) This ensures that management has covered all security bases (von Solms, 2000). Eloff and von Solms (2000) suggest system evaluation with process certification as an effective way of managing security. The authors argue that such an approach manages security from a holistic perspective of process and procedural domains. Standardizing the controls over a period of time will help the organization compare its practices with potential business partners. It also increases the trust and confidence of the external stakeholders. However, standardization has its pitfalls too. Such standards can only be viewed as baseline reference frameworks and might not be

adequate enough (von Solms, 2000) for all the contextual security needs of the organization. The variety of standards and their interrelations as well as the socio technical nature of the standards makes it difficult to achieve standardization (Hanseth et al., 2006). In conclusion, standardization of controls can be helpful if performed for repetitive and operational tasks. The task environment for routine business processes is less uncertain and the management aims at adhering to the same routine to gain efficiency. Standardization of controls for such tasks not only provides opportunities to improve it through benchmarking, but also gives opportunities to gain in productivity owing to these processes. We have argued against using standards "as it is" for overall security governance. Strategic processes and controls should not be standardized as it takes away the unique advantage of the organization and decelerates innovation.

Maximize Training and Education (M15)

Educating and training employees about the usefulness of control requirements ensures that users are aware of the controls, the risks and responsibilities involved in implementing the controls. Our data suggests that controls training programs could illustrate the relevance of controls with work related examples. Training with work related examples would be useful in understanding the depth and reach of the controls. Also, increasing awareness of social engineering issues is required. Education can be provided through regular training sessions about the need and usage of the controls. As shared by one of our respondents:

> Applying knowledge in daily practice is important. I think the training should be implemented in such a way that you not only develop the principles of security or privacy but also let them know its common usages and where they should be used

Our data suggests that regular training and education is good but should be assessed frequently for its impact on the trained personnel. Training should be enforced and the results from such efforts should be measurable in some way. As opined by a project manager from retail industry:

> How do you integrate your security and your development? If you have very standard mechanisms, then you can go for training. Hardly anybody goes for it. I haven't seen people going for security training, as it is not required. Interestingly. I do not think there is any additional cost to be incurred because the infrastructure is readily available.

Information systems security governance literature has long emphasized training and education as major components of security governance program. Lack of security control awareness is a major obstacle for effective information systems security governance (Johnson, 2006). Proper training and education helps in adopting a more congenial mindset and behavior towards security. Management should take measures towards increasing the awareness of the intent and scope of the controls. Education about controls is required for all levels of employees (Banks, 2004). Awareness about security issues and controls has many benefits in the long term. Some of the major benefits include (Johnson, 2006): increased customer confidence, better protection of confidentiality, increased reliability and correctness, fewer internal errors, early detection of security incidents, improved employee morale and improved compliance with laws. Organizational responsibility for controls varies from the top of the organization to the bottom. In a holistic approach, the organization has an unavoidable responsibility to educate all levels and functions in controls fundamentals (Banks, 2004).

Whitman (2003) suggests that employee security education, training and awareness program should be designed early on in the process of an information security strategy. This helps in increasing awareness of computer security problems and controls amongst employees' right from the very beginning. According to Warman (1992, p. 308), "It is essential for the success of any computer security policy that staff at all levels fully understand and implement the necessary procedures."

Newsletters can also improve employee awareness by publicizing new and previously unknown hazards. This also encourages employees to remain alert for up-to-date information and perhaps unidentified threats (Whitman, 2003). Consequently, education, training and awareness programs will create an organizational culture that will enhance, rather than compromise, security (Dutta and McCrohan, 2002). Understanding the perceptions of an organization's Board members with reference to risks and market expectations is another key to improving Information Security Governance (Ezingeard *et al*, 2003).

Ensure ethical and moral values (M16)

Ethical environment is essential for information security governance mechanisms to work effectively. Our data suggests that ethical and moral values tend to shape individual's perception about the importance of security control mechanisms and these perceptions lead to secure or un- secure behavior of the employees. It is important that the morality of the staff is encouraged and shaped towards respecting and conforming to the controls requirements. As explained by the systems manager, credit card services industry:

> Be aware of the morality of your staff. Allow them small things and don't wait for things like notices or bureaucracy.

Individuals often associate self pride with their jobs and this should be encouraged by the management. Self pride in the job actually shapes the work ethics in an organization which would ultimately help the controls culture in a positive way. As mentioned by an internal auditor, electronics industry:

> I would say that personal ethical and moral codes have a big role to play in security governance. Its very clear that people who are not honest or ethical, are not going to uphold codes which they think are useless and unnecessary.

Ethical environments where the strong moral values are communicated by the leaders of the organization tend to create a positive outlook about security governance and also a normative pressure on employees around to behave in a certain way.

Research literature in information systems security supports is appreciative of the role of ethics and moral values in shaping a positive security governance environment. Even though technical and formal means of security controls are important, these can only protect the data in the system. The contexts in which data is interpreted and used by employees keep changing and require broader normative controls to ensure that controls do work (Backhouse and Dhillon, 1995). Ethics and moral behavior is one of those controls. Dhillon and Backhouse (2000) argue that clear work ethics should be defined in work security environment as the types of data crucial to business are constantly changing. Policies, ethical and moral behavior should be communicated widely and clearly since this helps in formalizing the normative structures in an organization.

Maximize Trust building Mechanisms (M17)

Our data suggests that good security governance practices should be able to build trust relationships with stakeholders within and outside the organization. Given the nature of the job description in security work, it is crucial to win the trust of employees in order to ensure things run smoothly even in the absence of close supervision. One of the respondents, systems administrator and insurance industry spoke in this vein:

> We all must be capable of trusting everyone in the organization that comes into contact with our shared assets.

An environment of "lack of trust" and group politics, delineates people from the organizational objectives and a culture of "self before organization" creeps in.

As shared by a respondent, director IT services, state agency:

> Politics, favoritism, and self-interest typically trump values and may undermine the security of information systems.

Organizations should consciously try to maximize trust building mechanisms by ensuring clarity, transparency and accountability in actions. The role of the management goes a long way in shaping the trust building exercises. Management should work towards reducing the fears of the employees about unknown turn of events. This can be communicated through effective policies about sequence of events in case of deviation from the normal routine.

Research literature in information systems security suggests the importance of trust in effective security governance environment. Tsiakis and Sthephanides (2005) suggest that lack of interpersonal trust create ideal circumstances for a security threat. Trust and trustworthiness are fundamental for every security solution. The needs for trust elements and tools that are used to implement it, affect the security mechanism of any commercial

system. Ratnasingham (1999) suggests that role of trust is an essential element for long term ED1 trading partner relationships. The study suggests that trust leads to high performance via better trading relationships. In another study on trust and security measures, application interface was found to be important in terms of security. Trust needs to be established with outsider about the interface integrity and data protection via it (Johnston, Eloff and Labuschagne, 2003). Trust refers to defining the appropriate levels of norms and patterns of behavior that all members of an organization should be expected to implement (Dhillon and Backhouse, 2000). Trust is important for information security governance as sensitive data is often handled in the absence of close supervision.

In summary, the list of seventeen means objectives for information security governance is presented in the table 4.2 below. Under each objective, the corresponding sub objectives are shown. In summary, all the objectives developed in phase one of this study, are grounded in research literature.

Table 4.2 Means objectives for information security governance

	Objectives	Sub-Objectives
M1	Ensure Efficacy of Audit Processes	Develop audit practices for changing contexts of governance task Develop audit process to integrate the information rules Develop cross checking mechanisms for audit function Ensure adequate access to auditors across the organization Establish difference between audit functionality and actions Treat internal auditors as consultants to ensure effectiveness of controls
M2	Maximize clarity in business processes	Avoid improper business processes Establish clarity in business processes Understand the business processes Increase awareness of business activities and processes
M3	Ensure Communication about Controls	Communicate importance of controls Communicate the consequences of non compliance of controls Communicate the nature and scope of controls Communicate the consequences of internal controls breaches Encourage communication amongst employees about control issues

		Encourage debate amongst employees about control issues Encourage efficient communication policy within the organization Explain the purpose of controls Explain the rationale behind controls Explain the reasons behind organizational actions Explain the risks and values of controls to users Ensure damage assessment for individuals from lack of controls Ensure damage assessment to the organization from lack of controls Encourage discussion amongst employees about control issues Ensure responsiveness for media hyped issues
M4	Ensure Alignment of Individual and Organizational Values	Align personal and organizational values Align security control objectives with enterprise objectives Respect other people's confidence Respect other people's personal information Respect the rights of others Ensure employee satisfaction Ensure honor of the employees Protect self image of the individuals Change attitude of executives about security controls Understand people's attitudes and beliefs about controls Develop a result oriented attitude Develop people oriented controls Encourage determination about following controls Encourage dedication to the company Encourage individuals to improve controls Ensure that people see value in controls Ensure good values about security governance
M5	Ensure data criticality	Establish control structure to reflect sensitivity in data Assess the criticality of data integrity Assess the sensitivity of the information Define responsibilities according to level of confidentiality of information Identify data owners for sensitive data Link data owners with authorizations Ensure ownership of information Ensure adequate technical controls Develop identity management control Ensure confidentiality
M6	Ensure punitive structures	Set deterrence criteria to be followed Ensure action against unethical behavior Ensure disciplinary action against unethical behavior Ensure protection against disgruntled employees Ensure that action is taken against law breakers Establish clear consequences for not complying with laws Establish clear punishments for rule breakers Respect company's rules Encourage discipline in the organization Explain the disciplinary actions clearly Explain the consequences of failure to comply with regulations Explain the meaning of criminal action to the employees Create a fear of punishment in organizations

		Create counter measures to deal with destructive actions Analyze the psychology of the perpetrators Ensure environment of conformity that affects individual behavior
M7	Ensure clarity in control development process	Define multiple layers of controls Develop achievable objectives Develop controls as a part of the change initiative Develop controls for all the levels in the organization Develop simple and easy to use controls Discourage complex controls Ensure that control usage is simple. Ensure risks assessment to develop controls Structure the information needs Ensure that controls are easy to use Encourage flexibility in controls Ensure timeliness in controls
M8	Ensure formal controls assessment functionality	Institute controls as part of organizational design Discourage planning about control implementation as "after thought" Establish controls department Centralize the control functionality Develop security governance as a functional requirement Explain prioritization of tasks and actions for controls to members Establish the relation between controls and IT architecture Ensure IT architecture review for correctness of design Develop dynamic internal control structures Balance between gains and losses from the controls Balance centralization-decentralizations Balance convenience with usability Increase understanding of stakeholder viewpoints Ensure individual care to all stakeholders Protect company assets Avoid bureaucratic delays
M9	Maximize monitoring and feedback channels	Ensure adequate review of programs Ensure continuous monitoring of controls Ensure periodic review of controls from external auditors Incorporate feedbacks from people on daily basis Institute feedback channels for security governance Review controls with respect to organizational objectives Review the controls regularly for proper functioning Ensure the veracity of claims Institute corrective measures for continuous monitoring Encourage informal feedback from people about controls
M10	Ensure visible executive leadership	Encourage the management to "walk the talk" Encourage top management to lead by example Ensure respect for security leaders Ensure that key individuals enforce rules and remedial solutions Nurture relationships with employees Provide strong leadership Place committed IT personnel to be in visible positions Encourage control conscious attitude of supervisors Create an environment of leadership style and culture to minimize intergroup rivalry

M11	Maximize Group Cohesiveness	Encourage sharing the credit for good work Encourage the ability to share work Understand the group behavior driven by peer pressure Discourage favoritism in groups Discourage self interest in groups Encourage internal competition to stay within groups Encourage collaboration with peers Understand the influence of peer pressure on individual behavior
M12	Maximize management commitment	Ensure efficacy of controls through the management Ensure management commitment to controls Provide rewards for conformity with policies Discourage employee agitation Discourage impeding people from their job Discourage imposing ad hoc new rules Discourage providing all rights to an individual Discourage secrecy amongst employees Establish positive reinforcement for doing the right thing Ensure availability of the management Accord priority to the controls from the management Ensure that truth is told Encourage open mindedness to provide inputs. Reward good performance Provide recognition for complying with policies
M13	Maximize resource allocation for controls	Establish suitable environmental and physical controls Ensure adequate resources allocation for maintenance of controls Discourage individuals from feeling restrained due to resources Provide resources for compliance Encourage co-ordination between MIS and accounting for controls Establish controls proactively
M14	Encourage Standardization of Controls	Benchmark security governance investments against industry standards Benchmark security governance practices with industry standards Compare the state of controls with standards across the industry Establish standardization in the control process Refer to industry models and frameworks for control formulation Create systemization in the control development process Differentiate between lines of business. Differentiate between types of industry
M15	Maximize Training and Education	Define training programs to reflect details of internal controls Discuss the relevance of controls adequately Educate users regularly Encourage education about internal controls Ensure training with examples Illustrate with specific work related examples Ensure learning about internal control issues Increase awareness of breaches because of social engineering
M16	Ensure ethical and moral values	Encourage acceptable and respectable actions Encourage honesty Encourage access to individuals with strong moral values Ensure strong moral values in auditors Encourage personal integrity

		Encourage self pride in the job Understand the morality of the staff Respect personal integrity in a group Instill good principles into employees
M17	Maximize trust building mechanisms	Encourage trust building mechanisms for controls Establish trust in the organization Enhance an environment of trust in the organization Discourage an environment of fear Discourage an environment of mistrust Discourage politics in the organization Encourage free expression

4.4. Discussions

The first phase of this research proposed seventeen means and six fundamental value based objectives for information systems security governance. The objectives presented in the previous section have all emerged from our data. The means and fundamental objectives developed in this research have implications for information systems security governance research and practice. These contributions have been classified into three categories and each category is individually discussed below.

4.4.1 Relevance of the proposed objectives

The ISG objectives proposed in this research is not a stand alone effort but built on the cumulative knowledge in this area, above and beyond. Each objective proposed in this research is substantiated by the research literature. Some key lessons can be drawn from each objective. Table 4.3 presents the fundamental objectives proposed in this research with the research support and key lessons. On similar lines, table 4.4 presents the means objectives with research support and key lessons for practice.

Table 4.3 Summary of Fundamental Objectives

	Objective	Literature Support	Key Lessons
F1	Ensure Corporate Controls Strategy	Gregor et al. (2004); Peppard, 2001; Peppard and Ward, 2004; Alves et al, 2006; ITGI, 2006; Da Veiga and Eloff, 2007;	Control strategy aligns the security governance and business objectives Antecedent to complete security and process integrity Provides the departments with control plans
F2	Encourage a Controls- Conscious Culture	Julia and Westby, 2007; Da Veiga and Eloff, 2007); Dutta and McCrohan, 2002	Risk consciousness in employees creates a "prevention mentality" Helps in minimizing intergroup rivalry over security governance initiatives Creates environment where individuals "watch out" for each other
F3	Establish Clarity in Policies and Procedures	Ward and Smith, 2002; COBIT, 2007; COSO, 2005; Von Solms, 1996; Straub and Nance, 1990; Moultan and Cole, 2003; Cockcroft, 2002; Straub and Welke, 1998; Eloff and Eloff ; 2005; Tudor, 2000; McCarthy and Campbell, 2001	Ensure the proper use of the applications and technological solutions instituted Make policies easily accessible Reflect control requirements in the policies Develop visibility of fair policies
F4	Maximize Regulatory Compliance	Da Veiga and Eloff, 2007; Tudor, 2000; Eloff and Eloff, 2005; von Solms, 2006; Moultan and Cole, 2003; Dhillon and Torkzedeh (2006)	Meet legal, regulatory and contractual obligations Use compliance as a driver to develop security governance initiatives
F5	Ensure Continuous Improvements in controls	Booker (2006); COBIT(2007); COSO, 2000; Eloff and Eloff (2005); Rees et al. (2003)	Continuous and iterative control assessment improves the controls environment Understand the organizational context of particular controls Change in roles should be reflected in subsequent controls
F6	Enable Responsibility and Accountability in Roles	Pironti, 2006; Drummond, 2003; GISP security principles; Dhillon, 2001	Provide clarity in roles and ownership of decisions Promote transparency in roles and avoid sudden changes in responsibility structures

Table 4.4 Summary of Means Objectives

	Objective	Literature Support	Key Lessons
M1	Ensure Efficacy of Audit Processes	IIA, 2006; Drummond, 2003; Banks, 2004; Wagner, 2000; Trc`ek, 2003;	Have frequent internal and external audits Treat auditors as consultants to assess management's adequacy
M2	Maximize Clarity in Business Processes	Alves et al, 2006; Dutta and McCrohan, 2002; Moulton and Cole, 2003; Banks (2004)	Efficiently designed mature business processes are better protected Provide end-to-end view of business process and manage changes
M3	Ensure Communication about Controls	GISP, 2006; Leach 2003; CobiT, 2007, COSO, 2005	Have frequent debates about controls Develop communications policy for constructive communication within and outside functional groups
M4	Ensure Alignment of Individual and Organizational Values	Leach (2003); Jones and George, 1998; Baskerville and Siponen, 2002; Warman, 1992; Angell, 1996; Dhillon and Torkzedeh (2006)	Promote values such as respect for others, privacy, integrity, self-pride in job and honesty Involve users in the development process to understand individual's attitudes and beliefs about security
M5	Ensure Data Criticality	Volino, 2004; Finne, 1996; Sherwood, 1996; Ward and Smith, 2002, ISO 17799, 2006; Sandhu and Samarati, 1994; Booker, 2006	Assess and classify data according to sensitivity Identify data owners to assign responsibilities according to information criticality Link data with authorizations for secure and reliable IT infrastructure
M6	Ensure Punitive Structures	Dhillon and Torkzadeh 2006; Straub, 1990; Straub and Nance, 1990;	Establish clear consequences and disciplinary actions against non compliance with policies Explain the meanings of criminal actions and respond effectively in cases on non compliance
M7	Ensure Clarity in Control Development Process	CobiT, 2007; NIST 800-53-2, 2007; COSO, 2006	Develop a favorable perception and transparency of the controls Develop simple, flexible, timely and easy to use controls
M8	Ensure Formal Control Assessment Functionality	Ryana and Ryanb, 2006; Dhillon and Moores, 2001; Melling, 1994; Amer and Hamilton, 2008; Flowerday and von Solms, 2005	Develop formal entity for control assessment Differentiate between lines of business and industries before applying popular ISG frameworks Stakeholder's viewpoints needs to be reflected in the governance process Perform periodic cost benefit analysis and

			IT architecture review for correctness of design for the security controls
M9	Maximize Monitoring and Feedback Channels	Da Veiga and Eloff, 2007; CobiT (2007); COSO, 2006; Tudor, 2000; Dhillon and Mishra, 2006; Rees et al, 2003; Kolokotronis et al, 2002	Helps in achieving the performance standards set for the IT processes Assures "what is being claimed" is accomplished Incorporate the feedback into the controls
M10	Ensure Visible Executive Leadership	Julia and Westby, 2007; McCarthy and Campbell, 2001, Tudor, 2000; Eloff and Eloff, 2005; ISO 17799, 2005; Da Veiga and Eloff (2007)	Fundamentally helps in improving the perception of security governance Lead by example and nurture the relationships with employees executive
M11	Maximize Group Cohesiveness	Lepine and Dyne, 2001; Marks et al., 2001; Hogg and Terry, 2000; Kanter et al., 1992; Eloff and Eloff, 2005	Group behavior influences and shapes individual' perception about security controls Discourage favoritism and self interest in groups and manage peer pressure
M12	Maximize Management Commitment	Moultan and Cole, 2003; Ezingeard et al, 2005; ISO 17799, 2000; Von Solms, 2001; Kankanhalli *et al*, 2003; McCarthy and Campbell, 2001	Reward for conformity with controls and encourage values such as dedication, determination, open mindedness and truthfulness Establish effective controls as a "top priority"
M13	Maximize Resource Allocation for controls	von Solms (2000), ITGI, 2006; Dutta and McCrohan, 2002	Groundwork before developing controls requires coordination of multidisciplinary functions Allocate appropriate resources in politics free environment
M14	Encourage Standardization of Controls	Hanseth et al., 2006; Eloff and von Solms, 2000; von Solms, 2000)	Create systemization in control development process and assess against mechanisms employed by others Benchmark security investments and governance practices to learn from others
M15	Maximize Training and Education	Johnson, 2006; Banks, 2004; Whitman, 2003; Warman, 1992; Dutta and McCrohan, 2002; Ezingeard *et al*, 2003	Awareness about social engineering issues can be provided with work related examples Apply the knowledge in daily practice with focused training and education
M16	Ensure ethical and moral values	Dhillon and Backhouse, 2000	Propagate right ethical environment Leadership establishes the right tone of ethics in organizations
M17	Maximize trust	Ratnasingham, 1999;	Develop a conducive environment for

building mechanisms	Johnston, Eloff and Labuschagne, 2003; Dhillon and Backhouse, 2000; Tsiakis and Sthephanides,2005	controls deployment Enhance trust with partners within and outside the organization

4.4.2 Empirically grounded value based objectives

This research is presents a set of theoretically and empirically grounded information systems security governance objectives. A critical review of the extant literature for information systems security governance research suggests a lack of theoretically grounded information systems security governance framework. The popular security management standards such as COBIT, COSO, ITIL and ISO/IEC 27002 that are commonly used in practice are not without drawbacks. In the available models, there is neither any theoretical basis of the proposed objectives nor any of the frameworks proposed are grounded in data. The above mentioned models are atheoreical, anecdotal, generic and lack grounding in organizational context. Also, the above mentioned models are difficult to operationalize and implement because these frameworks need to be interpreted and bounded depending on the nature of the organization. As deliberated by a senior audit director at a fortune 500 financial services organization:

> COBIT is a pretty big model and very generic. It teaches you to think about what you have to think about. Look at COBIT and try to follow COBIT; you may need a lot of interpretation, it is going to be a long process. Companies have separate COBIT implementation project. It will help us greatly to look at that framework. You go to seminars to understand how it works, COBIT is way too much.

This research suggests 23 security governance objectives that are organizationally grounded in the context of controls. This study used "value theory" as a theoretical basis to

develop value based security governance objectives. The theory emphasizes the importance of values in human decision making and eventually behavior (Catton, 1954). The methodology used is a value focused approach which has been used in information systems research before (Dhillon and Torkzadeh, 2006; Keeney, 1999; Sheng et al, 2001, Drevin et al, 2007) but not in the context of information systems security governance. This is an important contribution to information systems security research and a stepping stone to take the work forward in this area. In information systems security governance literature, there is a lack of guidance on "how to develop security governance objectives?" In available security governance frameworks, not much light has been shed on how the suggested objectives were developed. This research suggests a value focused approach in developing decision objectives for information security governance.

4.4.3 Emergent nature of security governance objectives

There have been calls in the research literature about participative approach to security governance (Warman, 1992). In this "bottom up" approach, individual values are considered in developing governance objectives as it facilitates alignment of individual and organizational values. But none of the existing security governance models suggest objectives that reflect the values of the stakeholders. This research proposes value based security governance objectives. The process of developing a multi objective decision model using value focused approach has certain other benefits in addition to the direct benefit of creating better alternatives. Some of it's far reaching benefits include improving communications between stakeholder groups and providing systematic and transparent approach that often leads to uncovering hidden objectives (Merrick and Garcia , 2005).

Value focused thinking has been applied in many fields such as healthcare, waste management, transportation, port traffic management public health risk management (Merrick and Garcia , 2005; Keeney, 1992; Parnell et al, 2001).

Values are general standards or principles that are considered as intrinsically desirable ends (Jones and George, 1998). Considering that technological usage is influenced by the values and goals imposed by the executive culture (Schein, 1996), it is important to explain and reflect on the values of stakeholders for security purposes. People prioritize between various options and make a decision based on the relative importance of the values, which are their guiding principles (Rokeach, 1973). Value systems of individuals determines which type of behavior, events, situations or people are desirable or undesirable.

Butler (1991) argues that when people view something as desirable, their internal values strive to uphold the standard in behavior. For example an individual whose value system emphasizes loyalty and honesty will strive to achieve the same loyalty and honesty in work and personal life (Jones and George, 1998). Agreeing with the above researchers, we believe that values become all the more important in security governance context as the risk from circumventing controls can be catastrophic, a case in point being demise of the Barings Bank (Drummond, 2003).

In the context of security, organizations have to learn about new emerging threats and find means to deal with the threats proactively. As we know, organizational learning is the process of assimilating new knowledge into the organization's knowledge base (Abouzakhar and Manson, 2002). Organizational learning begins at the individual level. New individual knowledge is incorporated into organizational knowledge only when it is

shared and is assimilated into organizational routines, documents, and practices (Cohen and Levinthal, 1990). Incorporating the values of stakeholders into the governance objectives is important as beliefs and value systems may be used as mechanisms for strategic change (Marginson, 2002). As shared by a respondent:

> More and more businesses and government talk a lot about these personal values and train folks to understand the definition of the terms. What organizations fail to do is actively promote these same values by rewarding positive behavior and punishing unethical behavior [chief security officer, state agency].

This research provides a template for information systems security governance objectives that are rooted in the values of the stakeholders and provides an outlet for the opinion of individuals.

4.4.4 Synthesized information security governance objectives

The information security governance objectives presented in this research are grounded in literature and none of the objectives have been proposed for the first time. The above discussion on the proposed ISG objectives begs the question. "So what makes these objectives unique?" Research literature has presented much information security governance objectives in the past (see chapter 2). In practice, there are some leading frameworks such as COBIT, COSO and ISO/IEC 27002 which suggest ISG objectives based on experience and best practices across industries. But these frameworks for ISG do not suggest a comprehensive set of objectives that encapsulate all the dimensions of organizational governance in a single framework. For example, COBIT, COSO predominantly have formal socio-organizational orientation where the role of formal management is emphasized over the other aspects of security governance. Similarly, ISO/

IEC 27002 and ITIL have a technical orientation to security governance where formal, socio, ethical and moral dimensions are overlooked or under emphasized. We believe that these objectives are unique on several accounts. Their uniqueness lies in:

First, this research presents a synthesized set of ISG objectives which touches upon technical, formal, informal, moral and ethical dimensions of security governance, leading to a comprehensive internal controls program. While all our objectives have been generally recognized in literature (see table 4.3 and 4.4), they have not been presented cohesively as a synthesized ISG framework. This is a unique framework for ISG which incorporates several aspects of security governance into one platform thus allowing the development of a comprehensive security management program when implemented.

Second, the sub-objectives presented under each ISG objective clearly articulate the cross functional nature and multi dimensionality of the proposed objectives. Even though objectives by definition are generic in nature, the sub-objectives under the objectives so suggest specific directions for operationalizing a particular objective and putting it into practice. These objectives are more directive or prescriptive in nature. When implemented through appropriate tasks and activities, these would help in achieving the overall objective. Many ISG models in the research literature lack these powerful sub-objectives (see discussion on ITIL, COSO, Ward and Smith 2002, Booker 2006 in chapter 2) which facilitate the use and adoption of the objective.

Third, some of the objectives developed in this research have not been emphasized enough in ISG literature but potentially can play a crucial role in security management. Objectives such as “establish corporate control strategy”, “establish punitive structure”, “establish

clear control development process", "ensure formal control assessment functionality", and "maximize group cohesiveness" have been hardly designated as important for ISG in research literature. Thus the comprehensive nature of the proposed objectives provides a unique ISG framework for organizations.

4.5 Conclusion

Managing information systems security requires a holistic approach encompassing technical, organizational and behavioral aspects of security. The proposed information systems security governance objectives address risks to information assets from technology, processes and personnel perspectives in all facets of information asset environment. As Segev et al. (1998) note, the way towards security "lies not with technology, but with the organization itself". Effective information systems security governance calls for internal controls objectives that are grounded in organizational context and based on the values of the stakeholders in the organization. A common set of principles underlie all levels of an organization for any activity or objectives and is important to establish effective control (Galloway, 1994). In this chapter we have developed a set of security governance principles or objectives that guides the overall security program. The goal of this chapter was to present the data and the results of phase one of our study. In the beginning, a description of Keeney's three step methodology and the way it is used in this study was presented. The 17 means and 6 fundamental objectives which emerged using value focused approach are presented. All the objectives are grounded in the extant literature in the subsequent section. Having grounded the objectives, an overall discussion on findings and contributions of this framework is

presented. This phase of the research has produced theoretically and empirically grounded information systems security governance objectives. But the objectives developed have not been validated in an organizational setting to understand their relevance in real life. The validation of the developed objectives is addressed in the next chapter. A case study was conducted in the second phase of the research with two goals: reexamine the objectives in an organizational setting and interpret the relationships between various objectives to overall maximize security governance in organizations. The description of the case study site is presented along with the interpretations of the usefulness of the objectives in the particular setting.

CHAPTER 5 Reexamining information security governance objectives at CCIT

5.1 Introduction

This chapter presents findings of the case study that was conducted to reexamine the proposed control objectives of the previous phase of the research. An in-depth case study was done to understand the nature and significance of the developed governance objectives in an organizational context. The case study site was the information technology (IT) department of a major City Council (hereafter referred to as CCIT) in south east of United States of America. CCIT was chosen for the case study for two reasons. First, the organization is undergoing changes in its information security governance practices and is in the process of establishing new objectives, policies and controls for security. This seemed like a perfect fit for our purpose of examining the relevance of the proposed objectives in an organizational setting. Second, the management at CCIT was open to the idea of embracing changes in their ongoing security governance initiatives, based on the third party assessment of the state of affairs. A copy of this report would be shared with the organization.

This chapter has four goals. First, to establish if the objectives developed in phase one of the study is meaningful and relevant. Second, to examine how well the means and fundamental objectives help in explaining information security governance practices at CCIT. Third, to improve both the fundamental and means objectives in light of the case study at CCIT. Fourth, to comment on the security governance practices at CCIT, given our understanding of the proposed governance objectives. Each of these goals is achieved in the subsequent sections described below. The rest of this chapter is organized as

follows. The subsequent section presents an analysis of case situation in the light of the proposed objectives. The pertinent discussion about how CCIT is achieving each objective provides insights into the importance and relevance of the dimension of ISG vis a vis each one of these objective represented. The following section presents a synthesized understanding of how the objectives are relevant to CCIT. After establishing the relevance of the objectives, a discussion section is presented. The section shows how the objectives from phase 1 were refined and improved during the case study. It also documents the emergent issues at CCIT. Finally a conclusion section presents a summary of the case study and establishes the need for the subsequent chapter.

5.2 Context of the case study: CCIT

The City council (CC) is a state agency responsible for the administration of the city. The organizational goal is to work with customers to align business and technology objectives. A set of guiding values have been explicitly stated in the mission statement of the organization. Managing information security governance is identified as a strategic area of improvement by the agency. Security architecture at CCIT is focused in five areas: applications, authentication, networking & infrastructure, physical and process. The management emphasizes that improving security controls will drive efficiency and effectiveness across the city.

CCIT helps its citizens to receive more from the state government in terms of state of the art facilities enhanced by a strong information technology network. It also supports publicly accessible computers for free use by the citizens. The state uses an innovative technology planning process, which is driven by business needs of the state and aligned

with the city's business initiatives. The organization's CIO has implemented a new approach to create business technology plans. The strategic plan of the organization is to establish the common framework and processes that delivers IT services for each agency and establishes an enterprise view. The intent of such planning is to establish more enterprise level targets and evolve from agency focused goals. The benefits from such an approach are manifold. An enterprise approach by the agency reduces the costs of maintenance and helps manage enterprise level risks. Building common services leverages the resources and establishes effective partnerships between CCIT and other agencies. The organizational structure includes the CIO as the head of the agency. There are 5 managers who directly report to the CIO. The applications development manager is responsible for all the in-house development work. End user services manager is in charge of operations and support facilities. The infrastructure services manager is responsible for enterprise systems and database administrators. The manager in charge of administration is responsible for training and administrative support functionalities. The newly added project management manager looks after the software development projects in the organization. The organization overall has more than 100 employees at the time the case study was conducted, with several positions open for recruitment, as well as some consultants. The organizational chart is enclosed in figure 5.1

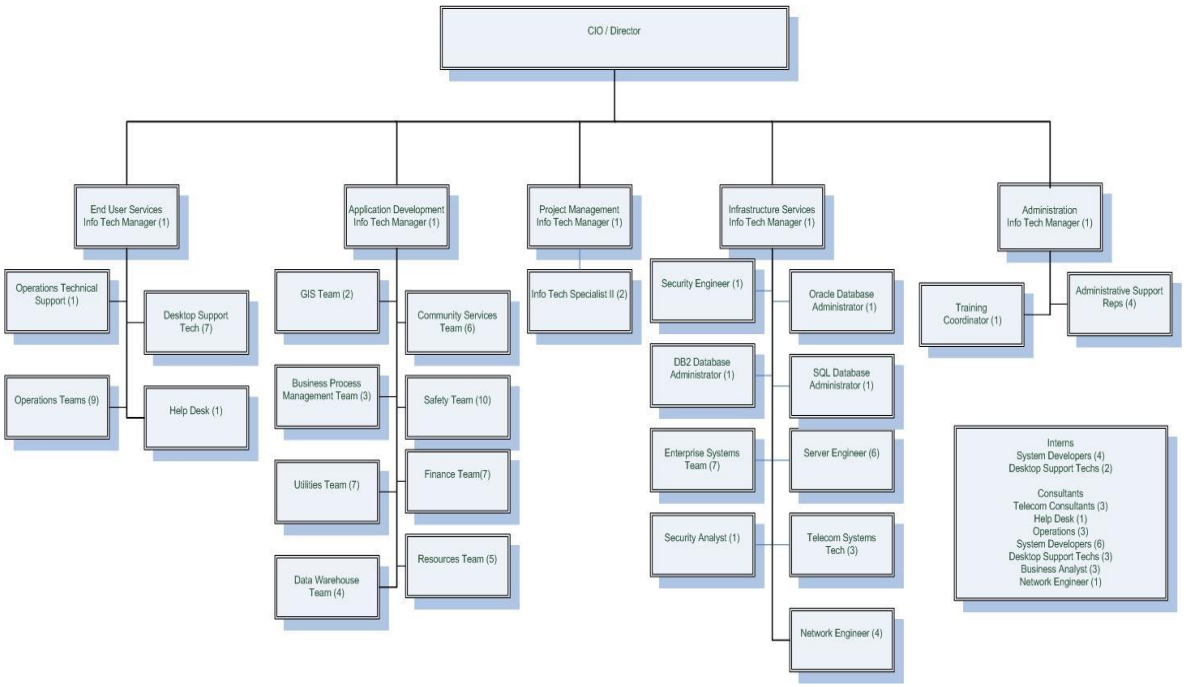

Figure 5.1 The organizational chart at CCIT

The technology planning process is tightly integrated and requires investment of resources from agencies and CCIT. Being the service IT provider for the entire state, CCIT has the additional responsibility of keeping the data and services protected. It is mandatory for the organization to keep its procedures auditable so that public scrutiny is plausible. The organization, having the ownership of IT services, acts as a service provider to all the other agencies supported by the state. To provide good infrastructure, the organization approaches every agency individually and assesses the agency's information needs and current state of technology utilization. The organization targets improvements based on specific needs of different agencies. These improvements are based on joint maps created with the IT organization and the agency.

The City Council is central to the information technology (IT) changes within the city. As IT evolves, it provides more and more ways to improve service delivery and operational efficiencies, providing valuable information for decision making and leadership purposes. CCIT plays an important role in the process of transformation of the ways in which business is conducted. The organization plays a strategic role in the way business is conducted in the city. The CIO of CCIT has initiated several task forces to implement changes to manage the IT architecture. The IT infrastructure is based on city's business needs and not on the latest technology trends.

5.3 How is strategic planning for information security governance being undertaken at CCIT?

The previous chapter proposed six fundamental and seventeen means objectives for maximizing information security governance. In order to understand the relevance, each of the objectives is reexamined separately in the context of CCIT. The objectives are used to explain the situation at CCIT, the measures taken by the organization to meet the objective and their impact on the overall security governance at CCIT.

5.3.1 Regulatory compliance at CCIT

This section discusses how regulatory compliance is perceived at CCIT and what is being done to accomplish it. Regulatory compliance, as a part of information systems security governance program, ensures that all the legal and mandatory requirements about security and internal controls are met in the organization. This objective entails formalizing the process of compliance in the organization and promotes development of controls in accordance with the legislations. Ensuring regulatory compliance is a fundamental

objective for information systems security governance. It suggests following the regulations in their entirety and using the legislations as a catalyst for the improvement of security governance.

CCIT as a state agency does not come under the purview of Sarbanes-Oxley act yet. But the agency has HIPPA and e-discovery as its main regulations to comply with. The agency has compliance audit, both from internal as well as external auditors. The culture in the organization is such that transparency about processes and availability of information are considered of paramount importance. The CIO is aware of people's right to ask for different types of information about the agency and use of taxpayers dollars in the operations. In accordance with state laws, most of the information about the agencies' current and future plans is accessible through the website. The common perception about the regulations and the compliance efforts in the organization is that of a "necessary evil". The middle level managers and the line staff consider compliance as the "right thing" to do but not necessarily helpful. This is understandable given the mammoth preparations required for compliance. Compliance with laws such as SOX is costly (Bennett & Cancilla, 2005). It needs managerial as well as technical support to create an infrastructure in organizations to meet the demands of this law. Some of the technical areas that need special concern for compliance purposes are: data management issues (Volonino et. al., 2004; Farris, 2004, Yugay and Klimchenko, 2004), security of data and system, choice of software development methodologies that could incorporate the compliance issues in its lifecycle, strong documentation for external auditing purposes, versioning and auditibility of electronic record needs and file systems in use (Peterson and Burns, 2005).

The internal IT audit director for the agency considers the regulations as something that are very helpful in providing a momentum to security and internal controls operations in their organization. This view is supported in the research literature as well. Myler and Broadbent (2006) argue that evaluation of compliance with the policies and procedures in an organization and regular follow up of the recommendations are important. The evaluation process helps in estimating the effectiveness and possible shortcomings of the controls process. Delineating audit controls and tools to determine areas for improvement (Myler and Broadbent, 2006) is what the IT audit director for the City believes in.

The chief agency head did not have a favorable opinion about the regulations though. As applications development manager commented:

> In my personal opinion compliance is reactive not proactive. You look at SOX. Enron collapsed and so many people were ruined or hurt and then SOX came. So compliance is a vehicle, the way compliance operates today, I don't think that an organization should say ok…we rely on compliance as a mechanism for developing our internal controls. If you do that you are going to be in bad shape.

This is an indication of the control consciousness and direction of the organization. The chief security officer is skeptical about the use of the regulations in developing actual controls. As he mentioned:

> SOX and HIPPA and other kind of things are to help protect data. But these are guidelines and they really don't mean anything by themselves because they don't come down and tell you specifically what you are supposed to do.

Internal controls are considered as something so serious that the organization should begin with these. At least this is what was apparent from our interviews. The general perception of the management about compliance is that it drives the security governance efforts

backwards. The regulations legislate something that should already have been a part of the governance program in the first place. This perception is consistent with the majority of research in this area. One of the biggest managerial issues that regulations imply is for IT governance purposes (Fox, 2004). Effective IT governance would require the management to plan for preparedness for quarterly reporting, security policies, cost management for compliance and preparation for external audit. These measures need planning and effective internal control assessment (Chin and Mishra, 2006). The management believes that the preparedness should be there to begin with and not inserted as an after thought while preparing to pass compliance.

Another interesting perspective about regulatory compliance came into light. Compliance acts as a huge driver in getting all the resources that are required for the agency. The security officer shared how in name of compliance, they order software, get management's attention and other required resources. The responsibility of the regulatory compliance efforts for the city does not lie with the agency. This explains a lot of discontentment with the use of regulations in the organization. Officials at CCIT just comply with the requests of auditors and supply all the paperwork required. The organization plays a passive role in the City's compliance plan.

Overall, it did appear to us that regulatory compliance is important for the agency. Since, the prime responsibility of being compliant did not lie with this agency; managers in the organization were candid about it. CCIT used compliance as a means to get things from the City which they would never get otherwise. Also, the organization is in the process of developing new policies and controls. It remains to be seen that how these new controls are

implemented and assessed. To sum up, compliance is important to CCIT but not in the right spirit of the legislations. A summary of regulatory compliance at CCIT is presented in the table 5.1 below.

Table 5.1 Regulatory compliance at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Ensure Regulatory Compliance	**"**SOX and HIPPA and other kind of things are to help protect those data but these are guidelines and they really don't mean anything by themselves because they don't come down and tell you specifically what you are supposed to do"	♦ Compliant with several legislations for state as well as federal ♦ Internal audit department guides through the process ♦ Develop controls proactively that easily meet compliance requirements

5.3.2 Ensuring continuous improvements in controls at CCIT

This section explains how continuous improvement in controls is achieved at CCIT. Instituting continuous improvements in controls implementation process has been identified as a fundamental objective for maximizing information security governance. The control implementation process should be iterative, continuous and adaptive in nature. The controls need to be changed over time and this should be reflected in the implementation process. Also, the importance of managing the changes in the controls is highlighted through continuous improvements. Effective implementation of controls calls for putting the right controls in right place at the right time and this can only be achieved through flexible implementation practices.

At CCIT, the management identifies the need for a constant reevaluation of controls under changing business conditions. Constant revalidation of the controls is very important for CCIT. As the Chief Security Officer shared:

> You have to keep up with it…It's not what you are getting over with…you have to constantly keep up with it…we do have some machines and software that are from over 10 years old…but you have to keep up with it….what else can we do..we need constant reevaluation as controls implementation is an evolving process.

This Chief Information Officer at the firm has a similar vision of regularly testing and updating the control structure. The importance of controls is appreciated in the organization and majority of the employees understand the need for a structure in place to accomplish the constant evaluation of the controls. The organization provides training and education to the security staff about the changing needs of controls and policies. The security officers are encouraged to attend conferences and seminars in the relevant area to keep abreast with the upcoming trends and technologies in security area. As one of the security officer said:

> I am a firm believer that you can put whatever you want in place but if the end user doesn't own it up, it is not going to work. I have been in seminars where I dealt with fortune 500 companies, people who are making billions of dollars a year as revenue and they still have the same problem. You know those guys have everything, they have done every thing but it [control implementation] needs to be a constantly evolving process. They have to learn and then reeducate because things change.

It was apparent from our observations at CCIT that the management understands the importance of the controls implementation process and maneuvers ways for everyone in the city council to be on board with it. There were frequent meetings and seminars about security controls and discussions on how controls should be used to overcome common security breaches. We felt a clear disconnect in the attitude of the managers and the operational people, about continuous changes in controls. The knowledge about the

benefits from revalidation of controls is concentrated more on the management side than on the operational side of the organization. The line staff and the non security people did not have much of an opinion on this issue. The non security folks considered control implementation as a technical requirement for the organization and clearly distanced themselves from the domain. The perception in the non security staff, working in development or other IT related areas, is that control implementation is primarily the work of security staff. The majority of operational people believe that the security staff should be responsible for the success or failure of the controls.

The situation at CCIT is not unique and the reasons for such responses from line staff is documented in research literature. The non security staffs at operational level, do not understand the significance of the security controls and governance for overall success of the organization. The enabling value of security controls has to be clearly articulated. Benefits of security governance should be linked with business objectives so that the stakeholders see the positive impact of security on attaining profits, productivity and growth. Security governance can help in avoiding negligence and enhance strategic business goals hence acting as motivator for top management (Wright, 2007). Research on the conditions which are conducive to information security problems clearly shows that where there are inconsistencies, there will be security problems such as errors, frauds, privacy and violations (Wood, 2006). It is important to ensure that security controls and security management practices of the organization are regularly reviewed. Such reviews could lead to finding mis-configurations in the systems and identify areas where security protection is such that a single failure could lead to large exposures (Wilson, 2005). The

changes introduced should not be radical and introduced with caution. An effort to implement technical and physical information security controls without considering the culture in the organization could have disastrous consequences (Thomson and von Solms, 2006). A summary of how continuous improvements in controls are being done at CCIT is presented in table 5.2 below.

Table 5.2 Continuous improvement in controls at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Ensure continuous improvements in controls	**"**We need constant reevaluation as controls implementation is a always an evolving process" "I have been in seminars where I dealt with fortune 500 companies, people who are making billions of dollars a year as revenue and they still have the same problem. You know those guys have everything, they have done every thing but it [control implementation] needs to be a constantly evolving process. They have to learn and then reeducate because things change"	♦ Constant reevaluation is done ♦ Considered an iterative process ♦ Attend seminars and conferences and learn about implementation practices form others ♦ Involve people across discipline and other agencies under city, to help in implementation

5.3.3 Responsibility and accountability structures at CCIT

In this section we discuss how CCIT assigns responsibility and accountability for security governance? Responsibility and accountability structures ensure that roles are defined in a way that appropriate responsibilities are shared and stakeholders are held accountable for their actions. This is identified as a fundamental objective for information systems security governance. The objective prescribes that job descriptions should be not changed abruptly, clear organizational responsibility for compliance should be defined, individuals should be made responsible for appropriate accesses and transparency about the accountability should be encouraged.

The management at CCIT completely identifies with the criticality of having clear responsibility and accountability structure for information systems security governance. The Chief Information Officer said:

> If you are talking about the outcome of the controls, then to me, its management. The idea of having a documented hierarchy especially around data is a must. If you think about it; we publish corporate organizational charts all the time. We should have a controls organizational chart which says, okay, if you are at this level, this is what you get [controls].

The CIO believes in the concept of having a "controls chart" which is similar to the organization chart. The controls chart clearly defines the responsibilities for the members regarding security controls. The controls chart is like adding control responsibilities to the organization chart. It helps in documenting the requirements for a role in owning up the responsibility of controls. As we go up in the controls chart and the roles become more crucial for security governance, the individual higher up should have more controls and accountability associated with their work. Research in security governance suggests that increased awareness and individual accountability can greatly affect how security practices are implemented in an organization (Mellor and Noyes, 2006).

The concept of a controls chart, as suggested by the CIO, is that as one moves further move up in the chart, the individual has more power in the organization. People higher up in hierarchy have greater accessibility to sensitive data and have greater probability of creating vulnerability in the system. Mellor and Noyes (2006) found that adding personal accountability into the roles helps the cause of security governance. The concept of controls chart is not implemented yet at CCIT, but would definitely be helpful for security governance purposes. As explained by the CIO, it is important to understand what is it that

we want to protect from a management point of view. If there is clarity in responsibilities and roles, better controls can be associated with the position and the individuals. For example, if the human resource people have high level of access to crucial personal identifiable data of personnel in the organization, there should be stringent controls for people in this department. As suggested by the CIO, such managers should be audited for their access pattern on a quarterly basis just to ensure that the managers are doing what they are supposed to do and security is not being compromised. Given the nature of the sensitive information that human resources people have access to, it makes sense to have better protection and accountability for such people. Research literature suggests that top management should be proactive about responsibility assignment to roles. Myler and Broadbent (2006) argue that corporate boards that undertake the challenge of plugging IT oversights show that they understand the scope of their corporate accountability and responsibility, and are proactive in their leadership duties. If organizations do not ensure that all employees understand their information security roles and responsibilities, it may become difficult to protect the confidentiality, integrity and availability of information assets (NIST Special Publication 800-16, 1998).

CCIT has access to crucial data about the taxpayers in the City. The department has access to DMV data, readings for gas, water and electricity consumption, property details and tax details about the residents. One of the duties of the department is to ensure that the meter reading for the household utilities is performed correctly as and when required. This operation, if not performed correctly, could present serious threat to integrity of the data recorded. As mentioned by the end user services manager:

> I think the accountability piece is required. How do they control, say even a meter reading application? How do we insure that every meter gets read every morning? You have meters that haven't been read and there has been no consumption on that meter for over a year and the service is still on, then there is a problem. So put controls and make someone accountable, that's how you guarantee that every meter is being read and the consumption of gas and water is recorded.

Reading utilities meter requires that there is appropriate segregation of duties defined in the organization else the security of the data could be compromised. It is essential to separate developers who make the application from people who actually read the meters and record the consumption by providing logical access to the groups. Else, it is possible for the developer to enter the application and change the readings for themselves or friends or whoever they deem appropriate.

At CCIT, management is concerned about assigning appropriate responsibilities and accountability to users of the systems. But it seemed that there is a lack of clarity of roles and responsibilities on many fronts. For example, when discussing the regulatory compliance issues in the organization, there seems to be confusion about who in the city council was actually responsible for the meeting compliance deadlines. People at CCIT meet auditors' request for submitting required documents. No one is sure as to who is finally responsible for putting everything together for compliance. A summary of how responsibility and accountability is being ensured at CCIT is presented in table 5.3 below.

Table 5.3 Responsibility and accountability in structures at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Establish Responsibility and Accountability Structures	"The idea of having a documented hierarchy especially around data is a must. If you think about it; we publish corporate organizational charts all the time" "So I think accountability piece is required. How do they control, say even a meter reading application? How do we insure that every meter gets read every morning? You have meters that haven't been read and there has been no consumption on that meter for over a year and the service is still on, than there is a pr	♦ clear segregation of roles ♦ developing a controls chart with clear control responsibility and accountability ♦ encourages ownership of information

5.3.4 Corporate control strategy at CCIT

This section examines how the corporate controls strategy is accomplished at CCIT. Controls could be a part of the bigger corporate strategy and security governance should be incorporated as subset of bigger picture of corporate strategy. This objective suggests establishing a corporate risks management plan and developing controls guidelines using consensus. Clearly controls should be viewed as a cost of doing business and developing control plans for every department. Security controls should be a non-negotiable budget item and adequate planning for the governance initiatives should be ensured. A control strategy establishes security governance as an antecedent to complete security and process integrity.

The management at CCIT believes that long term strategic planning is required to establish a security governance program in the organization. They need to have a clear vision about the security governance and each department should actually have its own controls plan and an enterprise level risk assessment plan. An information security risk assessment is the staged process by which an organization's information assets are valued. Here, the

vulnerabilities and threats are identified so that they then guide the implementation and monitoring of control strategies and measures (Whitman and Mattord, 2005).

At CCIT, there is a lack of agreement between stakeholders on what controls should be put and how should the controls be deployed and monitored. This disagreement is a direct result of a fundamental lack of planning and understanding about what are the assets and what is that actually needs to be controlled. A controls strategy can actually provide a broad vision for the organization in this regard. As shared by security manager:

> People should try to at first establish and see what the controls are. That's reflected in your requirements to some degree. People need to know what they want to control. You have to know what you want to control and the problem is that you don't know what you want to control.

The basic process of controls development approach needs long term planning and undying commitment on part of the management. The upper management seriously feels the need for a strategic planning approach for the security governance program in the organization. As shared by the infrastructure manager:

> I think that the design has to be around not necessarily verifying every single account but identifying what is the exception. What are the things that are causing the organization pain today? Where is security lacking? Where is money lacking? Where are people lacking? Where is time lacking? Why are the services not being delivered according to what we agreed with the customers? So you need to strategize about this stuff [controls design].

The CIO believes that if a strategy about controls needs to be established such that all pieces of governance program comes together. As explained by the CIO;

> You need to plan ahead and have strategy about controls and its success. You need to figure out how am I going to be proactive rather than letting a reactive compliance approach drive my internal controls that we use.

Our observations at CCIT suggest that a "bottom up" approach of developing security governance objectives would not work in this organization. The operational level management does not have a holistic picture about the role of controls in achieving overall organizational objectives. The strategic inputs about security governance should flow from the top management to the entire organization. Research literature is supportive of this role of the top management in control strategy formulation. Governance objectives cannot be decided from a bottom up approach. The lack of a control strategy would cause the, controls to be laid without risks analysis and policies. This could provide expensive and detrimental. With a top-down approach to management, a more appropriate strategy in the shape of long-term policies, efficient procedures and technical safeguards could be developed (May, 2005).

There are certain issues that do need strategic interventions for the betterment of security governance at CCIT. For example, there is a serious lack of planning about protecting the human assets in case of an emergency such as fire or flood. Without a sound strategy, efforts will be wasted. Therefore, a structured methodology for developing a strategy will increase the likelihood of success of the corporate initiatives (Shupe and Behling, 2006). We believe this is a serious strategy issue where the management at CCIT and at the City at large should think about: what is our strategy about protecting employees and equipments in case of emergency? The management at CCIT seems distressed about the fact that the City does not consider this issue important enough to discuss at high level

meetings. The state of affairs at CCIT does substantiate our call for a controls strategy which could plan about things such as this at corporate level.

Research literature in this area suggests that effective information security risk management processes should ensure that information assets are protected through selection and implementation of most effective control strategies (HB231, 2004). There is a growing awareness of the need for such a strategy (Shedden et al, 2006). Information security should be integrated into an organization's overall management plan (Lane, 1985, Smith, 1989). Firms have to integrate the IT strategies with organizational strategies to attain business objectives (Lainhart IV, 2001). In case of CCIT, the management could have an oversight committee that sets an appropriate strategy for IT governance endeavors (Myler and Broadbent, 2006) especially about the security events. A summary of the control strategy initiatives at CCIT is provided in table 5.4 below.

Table 5.4 Controls strategy at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Ensure Corporate Control Strategy	"People should try to at first establish and see what the controls are. That's some degree reflected in your requirements. People need to know what they want to control. You have to know what you want to control and the problem is that you don't know what you want to control." "You need to plan ahead and have strategy about controls and its success. You need to figure out how am I going to be proactive rather than letting a reactive compliance approach drive my internal controls that we use."	♦ Provide more resources ♦ Enhance trust ♦ Proactive controls approach versus reactive approach ♦ Corporate level planning for security governance in advance

5.3.5 A Control conscious culture at CCIT

In this section we discuss how CCIT nurtures a controls conscious culture in the organization. A control culture ensures an environment where individuals 'watch out' for each other. This fundamental objective emphasizes the importance of a control culture that

creates and sustains connections among various security efforts such as polices, processes and norms. A "prevention mentality" promoted by the control culture of the organization, helps in minimizing the friction between groups over security issues. It is important to establish standard codes of conduct for the employees in carrying out their security responsibilities.

The CIO of the organization believes in establishing a culture that needs to consider all the information that CCIT has and protects it as something personal for the employees. The CIO explained:

> I think you need to have a clear core value; a clear company recognized or accepted perspective, the role of having those controls. For example in my mind I think you should treat everything, every data you handle like its your information. Would you leave your wallet out in the middle of the street, on the bench when you go to get a coffee? what type of care would you take if it's yours? That is the kind of care you need to take.

Management espousing similar values as it claims should ultimately lead to the *shared tacit assumptions* of employees becoming aligned with these *espoused values* of the organization, thus progressing towards an Information Security Obedient Culture (Thomson and von Solms, 2008). The management realizes that it is a long and tedious process before a control culture is actually established. As the chief security officer enunciated:

> Establishing the concept [importance of controls] takes much time and commitment, to do that you want to bring that culture and it takes time and it is just a matter of time and that it will come, after you do it for long.

The management feels that establishing a control culture would help the policies and procedures in being followed properly and the management becoming more involved in the security governance process. The implicit knowledge of information security practices and procedures and the resulting behavior guides the day-to-day activities of the employees in the organization. As a consequence, information security practices and procedures should become part of the corporate culture of an organization (Thomson and von Solms, 2008). Culture is the glue that holds together various pieces of the puzzle and is a very important objective to be achieved. Speaking in the context of the culture, the desktop support manager commented:

> we can not have controls every where but should have control in the places where we can get the most benefit for the organization

From our observations in various meetings and even informal conversation with the employees, we did not feel that the organization had a control culture where people treat the information as they would treat their own property. Maybe it is the beginning of the long and tedious process of establishing a control consciousness of this nature because the leadership at the organization did seem determined to drive the organization towards control culture. There is evidence in the literature that suggests that instituting an organizational culture for controls is challenging, but important nonetheless. The controls culture is crucial for security governance as it can act as a powerful, underlying set of forces that establishes individual and group behavior within an organization (Schein, 1999). Ideally, a corporate culture should incorporate information security controls into the daily routines and implicit behavior of employees (Thomson and von Solms, 2006). If the

beliefs and attitudes are addressed by the management, it leads to changed actions and behaviors of the employees and synchronizes it with the overall corporate security culture in the organization (Thomson and von Solms, 2008).

Table 5.5 Controls conscious culture at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Establish Control Conscious Culture	"I think you need to have a clear core value; a clear company recognized or accepted perspective, the role of having those controls. For example in mind I think you should treat everything, every data you handle like its your information. Would you leave your wallet out in the middle of the street, on the bench when you go to get a coffee? what type of care would you take if it's yours? That is the kind of care you need to take" "we can not have controls every where but should have control in the places where we can get the most benefit for the organization"	♦ Environment where individuals watch out for each other ♦ Treat customers' information as if it is your own information

5.3.6 Clarity in policies and controls at CCIT

This section discusses how the management maximizes clarity in policies and procedures at CCIT? Establishing clarity in policies and procedures has emerged as fundamental objective for information systems security governance and has received extensive attention from researchers in this domain. This objective entails proper utilization of applications and technological solutions instituted in the organization by providing concise and consistent guidelines regarding its use. Policies should reflect controls requirements, fair, visible and easily accessible to all in the organization. Clarity in policies, communicates management commitment to security governance.

Policies and procedures are organizational laws that determine acceptable and unacceptable conduct within the context of corporate culture (Whitman and Mattord, 2003). It is a means to communicate management's commitment to the security

governance efforts (Myler and Broadbent, 2006). CCIT has a huge emphasis on establishing clarity of policies and controls. The common norm is to explain the policies and procedures frequently so that that it makes an impression on the user and stays with them eventually. Usually the most common reason why employees make mistakes about controls in the organization is the lack of understanding as to what needs to be done. Research suggests that good policies can protect vulnerabilities (Lapke and Dhillon, 2008). Better policies lead to deterrence as policies give the employees responsibility and accountability in the job (Maynard and Ruighaver, 2007). The security team feels that people never come up and ask about policies or controls unless they are in trouble. But to be preventive, the management at CCIT explains the purpose and scope of the controls proactively before the employees get into trouble. As the chief security officer explained:

> Make the policy and procedures clear and accessible. [Establish] Clarity in policies and controls, transparency in procedures and gradually standardization of the process, everyone knows what it could mean. What you [employee] can do to help & protect yourself without making those costly mistakes, make those very clear and understandable because if people don't understand them and they are not clear, people can't follow them and they make excuses.

The old security policies are not considered reflective of the current organizational needs; hence new policies are being developed. Research literature in security policy domain accepts the need for revisiting the policies periodically. For instance, it is becoming a huge problem to prevent employees wasting their time on browsing the Internet during office hours. Policies about personal use of computers during office hours needs to be clearly defined. Restricted Internet use or unlicensed software usage should be discouraged (Essex and Schauer, 2001). Maynard and Ruighaver (2007) maintain than besides the iterative

nature, security policies need quality verification periodically. This assessment needs to be carefully managed to ensure a balanced approach and make sure that stakeholders have adequate skills and training to assess quality. The management also believes that polices should be developed as a continuous process so that changing business needs are reflected. The infrastructure services manager commented:

> It's [policies and procedures] documenting and its following through. The key thing is documentation and it needs to be a fluid process, it's not static. You don't just do it once and throw it away, things change I mean. You had the best policy and procedure during mainframe but now you move to the Unix environment, that is no good.

The tax payers should actually be able to access the security policies in order to have confidence in the city's security measures about protecting their data. Also, the current policies have not been made easily accessible to the employees as well. This creates a potential rift in minds of people about the policies. As the security staff officer explained:

> We had regulation and policies established but did people know that? Make all the required things accessible to people. Our policies are so hard to find on our website that I don't know how anyone can ever read them. This is serious.

The management is developing a new set of security polices and procedures. It is planned that the security policies would be made accessible to all the citizens at the web site. A central repository of security policy and control resources would be created on the Intranet which would be accessible to all Agencies City wide. To establish the clarity of new policies, extensive educational sessions have been planned. It remains to be seen in the future though that how well these measures play out in establishing effective security

governance. A summary of how clarity of policies and procedures is being accomplished at CCIT is presented in table 5.6 below.

Table 5.6 Clarity in policies and procedures at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Maximize Clarity in Policies and Procedures	"Make the policy and procedures clear and accessible. [Establish] Clarity in policies and controls, transparency in procedures and gradually standardize the process, everyone knows what it could mean. What you [employee] can do to help & protect yourself without making those costly mistakes, make those very clear and understandable because if people don't understand them and they are not clear, people can't follow them and they make excuses".	♦ Explain the policies repeatedly ♦ Make the policies accessible easily ♦ Continuous iterative process of development ♦ Constant explanation of the benefits

5.3.7 How is efficacy of audit processes ensured at CCIT?

Auditing acts as a catalyst for the management to accelerate its efforts for information systems security governance. This objective is quite useful especially in the context of change management, to ensure segregation of duties in the organization. The underlying sub objectives point towards use of audit process for cross checking the business activities. Auditors should be treated as consultants for a third party perspective about risk management. Audit efficacy is required to assess management's adequacy with dealing with vulnerabilities.

The role of auditing in improving the effectiveness of security controls is well understood and communicated at CCIT. The top management emphasizes the importance of auditing culture in the organization and claims that it should be undertaken frequently and on demand. Research literature suggests various reasons for having frequent audits such as estimation of organizational preparedness, identification of vulnerable areas, benchmarking against standards and practices, and compliance with legislation (Goel et al., 2006). Audit

trails can be designed to help in intrusion detection. Real time auditing can also help in detecting other problems in the system other than break downs. Swanson (1996) argues that auditing helps in creating individual accountability, reconstruction of events, intrusion detection and problem identification. Audit provides traceability of user action and chain of evidence can be reconstructed to actually understand when and how the system broke down (Goel et al., 2006). The need for frequent internal audits was felt all across the organization and not just the security group. The HR manager said:

> You got to have some body audit behind them [employees]. You got to have separation of duty and segregation of duty. Cross training is great, if works. How do I control who should do what if I m not going to watch it?

The administrative manager at CCIT believes in cross training her team members for a variety of roles such that the work does not stop in an individual's absence. But the auditors enforce segregation of duties so that no vulnerabilities are created in the processes because of interchange of the roles. Thus the auditing functionality helps in ensuring appropriate role design at CCIT.

The perceived role of auditing at CCIT is to provide assurance about the quality of controls that are in place and effective. The management believes that auditing "gives them a meaning for doing things". Even though the medium of business transactions have changed from paper format to electronic data, the traditional wisdom accrued from auditing and accounting standards is still valid. As commented by one of the managers:

> I think auditing provides quality assurance which is very important. If you don't have audit you have no compliance. Right now, you have to audit because all the process are not automated, you can't expect control at every single process. I

> think 60% of all processes here don't have any electronic support or computers at all. People do the work, so we have the audit.

The general perception in the organization is that audit helps in establishing and enforcing punitive structures. It is a means to ensure that people keep doing what they are supposed to do or else they would be penalized during auditing phase. Also, auditing is increasingly being viewed and accepted as a requirement for regulatory compliance preparations (Fox, 2004). Frequent audits help people in perform their jobs within accepted boundaries and ensure that organization is geared up for compliance purposes. As explained by the infrastructure services manager:

> They [auditors] make people honest. If you know someone is watching and will look at what you are doing, you know it makes a difference. Even if you don't look, 90% of the time just the threat that you are going to be looked at, you don't know when, makes a big difference on compliance. I would like to say human nature is such.

At CCIT, there is an apparent contradiction in what management believes that should be done and what it actually does about auditing. In theory, the management unanimously agrees to the importance of internal auditing functionality and its benefits for security governance in the organization. But in practice, there are fewer number of audits than we expected. One possible explanation of this contradiction could be that there is an underlying sentiment in the organization (as gathered from various informal discussion and observations) that usually in a government agency, auditing is perceived as a tool or excuse to "get back" at someone or some department i.e., to punish them for some unrequited act. The under current is that if the boss is unhappy about something from an agency, that

agency faces the brunt by getting frequent audits. As shared by manager, "We got to get over the idea that auditing is not losing control. Auditing is to keep us on top of things". It remains to be seen though that in the new security policies and controls that are under the way, what role would be provided to the auditor in the security governance framework. But as of now, CCIT gets very few internal audits and fewer security audits. A summary of the audit efficacy initiatives at CCIT is presented in table 5.7 below.

Table 5.7 Audit efficacy at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Ensure Efficacy of Audit Processes	I think that if I took over, if I became the CIO, I would be looking at every one of my team members and I would tell them to prepare for an audit. I would bring an auditor here and each one of my team will get audited. That would give me a base line as a new boss to work on, I can only improve. If it got any worse my job should be gone that's what I would do. Management should be responsible for what's going on. Economy improves if the government works.	♦ Management believes in frequent audits ♦ Use audit as a deterrence tool ♦ Used to provide quality assurance ♦ Helps in keeping on top of things ♦ Audit on demand

5.3.8 Communications about controls at CCIT

This section describes how the management communicates about controls at CCIT. Communication about controls is important to articulate the vision of the management about security and establish a constructive debate about the usefulness of such activities. It pays to clearly establish the intent and the scope of the controls and this can be achieved through open and constructive communications. Frequent discussions, not only within the security and control groups, but also with other functions in the organization, establishes a clear baseline of expectations from the employees and prevents unintentional breaches. The management at CCIT is serious about communication with the employees regarding controls. The CIO has an informal meeting on every second Friday with the employees

where the pertinent issues about security and controls are discussed, employee feedback is taken and agreement on future course of development is reached. The chief security officer adheres to the following principle about communicating with employees:

> Make things very clear to the employees, these are our policies, these are our procedures and controls and these are our expectations. It is essential to communicate this.

The management has a preventive mentality and clearly wants to protect people from creating vulnerabilities in the system. The accepted point of view is to communicate the controls in a clear and concise way so that people understand the expectations. Consciousness-developing communications helps employees to identify with the organization and the work that they do in groups. The security officer explained:

> The best time to do that [communicate] is during orientation, a sound understanding of what is expected from you [employee] and how things happen. I prefer accent on the positive rather than on negative thing. It doesn't mean that consequences shouldn't be mentioned but I think rather than emphasizing that part let's emphasize procedures and the prevention because that's what you really want. You don't really want to punish people for mistakes who have done something wrong. You want to prevent somebody from the beginning.

The emphasis on communications about controls stood out clearly, in our observations, through the actions of the management at CCIT (see table 5.8). Research literature in information security governance emphasizes the role of communication in the success of governance program. Fuller et al (2007) suggest that there exists a positive relationship between interactivity and knowledge retention about information assurance in an organization. The interactivity is best facilitated by open communications. Communication activities with stakeholders are critical for controls (AS/NZS 4360, 1999). A good way to achieve communications is through the standardization of controls. At CCIT, in the

process of the development of new security policies and controls, the management held meetings with employees' representing other non security expertise areas, and took their feedback on what were the most important issues for the security of the organization and the city. A list of priorities was decided based on the feedback from this meeting. The management proceeded with requisite actions in the direction agreed upon in the meeting. Thus management at CCIT is open about communications and feels that it pays to communicate, even when the payoff is not apparent immediately. The HR manager observed;

> They [employees] like to know the reason, why? They like to hear things. People may not communicate to us but people like to be communicated to, it may not go both ways all the time but in my experience I found that people like to be told

Even though the communication culture seems strong within the organization, there is a lack of communication between the organization and other agencies under the City about the security policies and the controls. Organizations clearly communicate values and visions such that employees can internalize it and make sure that it is synchronized with their own (Wright, 2007). But this is not true for the directors working for the different agencies at the City. The fate of the newly developed security policies depends on the committee that comprises directors from other agencies under the City. It requires a lot of communication between these directors and CCIT to actually establish what policies the City needs and should be signed and made official. Evidences from research warn about such situations in organizations. Poor communication is itself a security risk (Wright, 2007). It allows security policies to be misinterpreted, security messages to be

misunderstood, and ignorance about real security threats is cultivated. Communication is essential for a proper security governance program. But there is lack of communications partly because of the group dynamics within the City council. It is to be seen in the future how this communication gap would be addressed by the CIO of the organization in order to facilitate the efficacy of the policies.

Table 5.8 Communications at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Encourage Communication about Controls	"Typically in our case, we would draft a policy, edit it and go to city. Managers and other directors from other agencies need to work on this but there is no communication among them. So there is no feedback. If there are thing that you don't agree with, tell us, we need to get there input. They need to be treated differently, they are different departments".	♦ Meetings with employees every second Friday ♦ Communicate with people even when they communicate back ♦ Prevention is better than creating vulnerability hence communicate to protect the people

5.3.9 Data criticality at CCIT

This section explains how data criticality is achieved at CCIT. Establishing data criticality has emerged as an important objective for maximizing information systems security governance in an organization. Establishing data criticality entails assessment and classification of data according to sensitivity, identification of data owners and assignment of responsibilities according to information criticality. Maintaining the confidentiality, integrity and availability of the data is not only required for securing business processes but also needed for regulatory compliance purposes. Linking data with authorizations helps in creating secure and reliable IT infrastructure. This is one of the most prevalent security governance objective, both in research as well as in organizations.

The core business for CCIT is IT service delivery to other agencies under the City. Since CCIT forms and supports the backbone of the IT infrastructure for the City, it is imperative that the organization ensures protection of critical data and make it available to all. The chief information security officer explained:

> We do have data that is crucial. We may have health data, we may have social security numbers and the names and dates and all of those things. Also employee details that we need to keep private as well. We interact with other state agencies and there is other information. We have access to DMV that means details of basically any body who owns a car, so lot of data. We must ensure that data doesn't go anywhere where it shouldn't be, so from that point this is what we are going for. All of the IT security controls are really all about the data.

Maintaining the criticality of data is absolutely essential as CCIT acts as the custodian of all sensitive information about the City. Being the centralized IT service provider to the entire City, CCIT prides itself on providing a technically superior state of the art service centre with 24/7 hotline and helpdesk services. A compelling need for data security at CCIT is materialized through stringent access control and authorization mechanisms. Research literature suggests the importance of establishing data criticality through security governance mechanisms (Finne, 1996; Sherwood, 1996; Ward and Smith, 2002). Security controls are important as assurance hinges upon the integrity of the critical underlying IS change and configuration management processes (Hinde, 2006). At a higher level, even security strategy is incomplete without planning for measures to safeguard data integrity (Tickle, 2006). A control strategy about data criticality provides users with confidence in the integrity of data and the end result is trust in the IT infrastructure, really valuable in

today's business world (Tickle, 2006). The management is appreciative of strict controls for access data. As mentioned by desktop support technology officer:

> I think that what you would have to do is that you force the system to make them [employees] doing things. If a person doesn't change his password, in thirty days, he gets locked out the system. Don't allow them to fool around.

The management at CCIT feels that developing controls for proper access of data requires adequate segregation of duties. Separation of development, test and operational facilities helps in reducing risks of unauthorized actions (Myler and Broadbent, 2006). The director for internal audit asserted that it is critical that people on the development side of the environment, ones who write the actual codes for the applications, do not have access to the production environment and that each and every change in the production environment is documented and logged properly for audit ability purposes. As explained by the chief internal auditor for the City;

> Security controls are revolving around data, the ability to keep integrity of the data. It [controls] revolves around internal and external access of the data. In processing all sorts of access there you want to make sure that all the access is limited to the data somehow there is need to for a segregation of the production data and that is accomplished in many-many ways.

The security team also checks the external access devices for security purposes. The security team feels that even if there is a modem which is not very prevalent, let loose on the network somewhere, it could become a threat. It is crucial that only authorized people get access to authorized sites which include databases and other parts of the network. To ensure that the access rules are designed properly, frequent audit is encouraged. This helps in tracking the vulnerabilities in the systems and taking action about the weak points. As mentioned by the Chief Internal Auditor:

> There are several tests that a security auditor would perform such as penetration test where the auditor would try and acts like a hacker and try to break into the network. If the auditor is successful he will uncover various vulnerabilities of the system and the network. The security people have to figure out how to deal with these vulnerabilities without opening additional vulnerabilities. Thus quality of network improves to the point that it becomes really good.

The management believes in good access control polices and even better authorization mechanisms. At CCIT, access is defined for the users depending on the sensitivity of the data. It is important to ensure that the person who has the appropriate access is the person accessing the data. The management emphasizes strong authorization mechanism, which tells us how important data criticality is to the management. Many managers feel that security governance is all about managing risks through right access to right people at right time and making sure that those very right people are getting the access through right authorizations. A summary of how data criticality is achieved at CCIT is presented in table 5.9 below.

Table 5.9 Data criticality at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Establish Data Criticality	"We do have data that is so crucial. We may have health data, we may have social security numbers and the names and dates and all of those things. Also e the IT security controls are really all about the data"	♦ ensures confidentiality, integrity and availability of data to all ♦ Provides a technically superior state of the art service centre with 24/7 hotline and helpdesk services. ♦ Segregation of duties ♦ Stringent access control policies ♦ Strict authorization mechanisms ♦ Strict password policies

5.3.10 Clear controls development process at CCIT

This section discusses how clarity in controls development process is established at CCIT. Clear control development process creates a positive perception about the controls and ensures transparency in control activities. This objective emphasizes the importance of systemization in control development process and defines achievable goals. Also, a balance between stringent and useable controls is desired, which can be achieved by structuring information needs for risk assessment to determine the scope of the controls. This objective encourages developing simple, flexible, timely and easy to use controls. Clear control development process helps in protecting critical business processes through multiple layers of controls as the requirements of such complex controls is evidently established for everyone.

The management at CCIT clearly believes in the importance of establishing clear control development process for information systems security governance. As one of the security officer said:

> Actually creating the policy and the procedure needs to be clear because if no body knows about the controls and procedures or understands it, they are not going to follow it.

Clarity in controls development processes is emphasized at CCIT. The management encourages employees to clarify any doubts about the policies and welcomes questions about them. The management has also created a channel through which such requests are formally processed and quickly responded to. The human resources department in this organization is responsible for enabling all the employees to get access to any resource that

the employees might need to understand the policies better. Also, it is encouraged in developing simple and easy controls that can be easily understood and quickly incorporated in daily work. As mentioned by the service engineer lead:

> You got to put it [controls] in a way that it's not complex, it's not complicated. So you put together a check list and put together a general list [controls]. More general the list, larger the deviation from what you want. You have to be specific but you don't want so detailed [controls]. You have to define how far you want to go. So if you want City's webpage to be the homepage, you got to define in that check list and make sure that it's [making City's webpage as homepage] one of the things you do.

Research literature in this area suggests ways to enhance clarity in controls development process. Dhillon and Backhouse (2000) argue that patterns of behavior must be well defined and explained thoroughly in company policies to enhance trust within the organization. This can be achieved only through clarity in development process for controls. Dhillon (2001) establishes the benefits offered by clarity in controls development process. He suggests that clarity in controls development process and incorporating controls in systems development would have better impact on technical controls and thus enhance data criticality. Controls, where possible, should be transparent or viewed as positive contributions to job performance. The extension of controls that increase constraints on people should be minimized (Parker, 1996). Mature organizations have well established and institutionalized processes which help in the segregation of duties and lead to effective cross checking mechanisms such as auditing.

The management's attempt to establish clarity in controls development process seems to work for the employees at CCIT. But with a change in policies and controls coming into

effect very soon, it remains to be seen how well the management is geared to help people understand these changes in controls structure. It would require a lot of planning and coordination to actually implement the new policies and controls effectively and establish the clarity of the controls in the minds of the employees, crucial part of the success. A summary of how that management encourages clarity in controls development process is provided in the table 5.10 below.

Table 5.10 Clear control development process at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Establish Clear Control Development Process	" Actually creating the policy and the procedure needs to be clear because if no body knows about the controls and procedures or understands it, they are not going to follow it"	♦ Encourages employees to clarify doubts ♦ Make all resources about controls accessible ♦ Simple and easy to use controls

5.3.11 Formal control assessment functionality at CCIT

Formal controls assessment functionality allows establishing security governance as a functional requirement. Security has always been considered a non functional requirement. But security cannot be represented only by nonfunctional requirements since security goals often motivate new functionalities, such as monitoring, intrusion detection and access control, which, in turn, need functional requirements. In addition, a distinctive feature of security requirements is that they are asset-driven – their goal is to protect the set of identified assets (Antilla, 2007). Having a centralized entity for controls assessment would allow separate budget allocation for security governance functions and help in establishing a business case for security governance. A controls department would integrate controls into the business processes. Formal controls assessment functionality also entails

establishing a relationship between IT architecture and controls, dynamic control structures, balancing centralization-decentralization of controls and encouraging job designs around information systems needs. A formal entity for controls in the organization also helps in avoiding bureaucratic delays for controls purposes, prioritization of resources and tasks and institutionalization of controls as a part of organizational deign. A security governance objective of this nature is not emphasized in the extant literature.

CCIT is in the need for a formal process or channel through which all its control related work is managed. It came up repeatedly during the interaction with the organization that controls should be treated in a way that other departments are treated. As manager of development puts it:

> I would say sign off on the requirements that the key stakeholders have agreed upon. Develop the feasibility metrics so that you can take each requirement and trace it through out the whole system all the way from requirement to functional design. This process has to be done formally

The budget and monetary considerations is a huge thing for the organization. At CCIT, money allocation at any step is heavily bureaucratic hence delayed. Resources for controls need separate budgetary allocation and this could be achieved through establishing a formal entity with separate budgetary needs. As shared by manager security;

> The biggest problem is that controls have limited resources. We want to do so many things but can't do it. Like it [controls] needs to be constantly modified and monitored but that [modification and monitoring] needs investment. Do we have separate money for this as a department? We are always in a cash crunch.

The chief security officer shared the similar view:

> You have to provide proper resources and assess the proper control requirements. Hackers are not fools, you cannot use off the shelf controls and put these in

> place and expect them to work. We can ensure that it works but we need resources for that and we don't essentially have those resources. To get the resources, it is helpful to have separate budgets.

The management feels that it is prudent to perform the cost benefit analysis to establish the worth for the investments in controls. Unless a business case in terms of cost and benefit is made, the directors up in the City council are hesitant to allocate resources for control purposes. The manager, enterprise systems team explained:

> Everything comes down to the cost of the risk. How do you balance cost of the control versus the risk? Risk is great; cost of control may be worth it. How do you balance cost of the risk to the control? It is same as security. You can make it so hard to get into the system such that they [employees] spend all day just to figure out how to get in, takes all the time and work is never done. That's obviously not the goal but protecting our data is very important

It is evidenced in research literature that cost benefit analysis for security measures is important to establish the credibility of the efforts. Cost-benefit analysis of access controls devices should be done periodically (Schauer and Essex, 2001) to understand the risks involved. It is critical for organizations to ensure the most effective and cost-efficient controls strategies are selected. The management also needs to ensure that balance in cost of controls, the level of security and access to the system by end users is achieved. It is important to bring various user management, permission and access control functions together and to investigate how technology can be deployed to simplify or centralize management, reduce costs and achieve higher levels of control, security and assurance (Wilson, 2005). This can be adequately done through development of separate controls

assessment functionality. Establishing an entity of this sort entails new requirements for the management.

Though it was not clearly articulated, the management suggested a need for centralizing all the controls initiatives for governance purposes, it remains unclear if any step towards this direction has been taken by the management. The job descriptions for individuals working in the controls assessment department could prove critical to security governance of the organization. Jobs dealing with confidential information should also have stringent hiring requirements and ensure that individuals being given these roles take their roles seriously and have an eye for details (Myler and Broadbent, 2006). It is important to remember that the control environment has a pervasive structure that affects all business activities such as management's integrity and ethical values, operating philosophy and commitment to organizational competence (Ramos, 2005).

Table 5.11 Formal controls assessment functionality at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Establish Formal Control Assessment Functionality	"The biggest problem is that controls have limited resources. We want to do so many things but can't do it. Like it [controls] needs to be constantly modified and monitored but that [modification and monitoring] needs investment. Do we have separate money for this as a department? We are always in a cash crunch" "Everything comes down to the cost of the risk. How do you balance cost of the control versus the risk? Risk is great; cost of control may be worth it. How do you balance cost of the risk to the control? It is same as security. You can make it so hard to get into the system such that they [employees] spend all day just to figure out how to get in, takes all the time and work is never done. That's obviously not the goal but protecting our data is very imp"	♦ Cost benefit analysis for controls ♦ Ensure resources ♦ Needs a formal entity for centralized controls management

5.3.12 Monitoring and feedback for controls at CCIT

Monitoring controls requires effective and established channels to incorporate feedbacks for further enhancements. This helps in achieving the performance standards set for the IT processes and assures the management "what is being claimed" is being done. Periodic review from external auditors strengthens the controls structure and helps in analyzing the alignment between control objectives and overall business objectives. Monitoring the controls and incorporating the feedback from employees into the controls structure has been emphasized by almost all the prevalent governance models (COBIT, 2007; COSO, 2003).

CCIT believes in strong monitoring and feedback channels for the success of information security governance. It has a monitoring program, for the most part, for all its processes and controls. Research literature in information security arena accepts the critical role played by monitoring and feedback process in the success of security initiatives. The post implementation monitoring and review of controls is a critical phase for success of overall controls program (Shedden et al, 2006). Another positive result of good feedback is improved communication between the management and the employees. Straub and Welke (1998) suggest that regular feedback sessions lead to better communications in organization. These values are communicated through departmental meetings, and informal chatting. CCIT also believes in getting regular backups of the data set as a result of routine monitoring process. The backups help the management stay in touch with performance of the controls in real time. Having backups ensures that not only the unauthorized use is prevented, but also continuous authorized use is encouraged (Schauer

and Essex, 2001). Regular backups should be encouraged irrespective of the storage cost as the benefit from recent backups is immense in case of a disaster. The HR manager is optimistic about the monitoring tools that she has in her department. As she commented:

> The system in which I am right now, I am in a place where I am able to find out what they have done whatever needs to be done, seeing the audit trail. If they haven't done their work, we find that pretty quickly

Monitoring the controls and using the feedback for improvement is the norm at CCIT (see table 5.12). The management understands the role of monitoring in the success of governance efforts and takes the responsibility seriously. As shared by manager:

> So the control has to be more than the lip service, some how it got to be enforced. There got to be some way to guarantee that if I give you access in security form, how we know he gave that access to the right person at the right time. Even if the person is authorized to do that, security controls are needed also about how things are being misused even when legitimate access is there

CCIT implements stringent authorization process and strict password policies to ensure that right people get the right access. The management follows the philosophy that the feasibility of the controls can be verified only through monitoring. Monitoring process validates that everything is being followed correctly and the feedback allows in assessing the feasibility of the controls. Feedback about the controls is encouraged at CCIT. As shared by the security manager:

> It's kind of like you want to go back and constantly go back to people and keep looking. Is this really working for us? Asking people if this is what they can work with is important.

It is evident that monitoring and feedback does consume resources at CCIT. The effectiveness of monitoring techniques and policies requires employees' willingness to

comply with their use (Booker and kitchesn, 2007). Insights into employees' intentions to comply with policies or circumvent monitoring tools are helpful in promoting effective use of these technologies. The insights can be drawn from the feedback received. Monitoring is taken seriously and performed frequently. So is feedback from the operational level employees. The management at CCIT strives to create a controls culture where monitoring and feedback are valued in the organization. However, with forethought and purpose to build a culture of trust, employees will be more likely to embrace the need for monitoring techniques that prevent criminal and negligent activity (Fleming, 2007).

But it is not clear that what is being done with the feedback? It is one thing to take feedback about things and make people involved in the process. The fact that employees get to voice their opinion of controls could actually make them feel empowered and hence more receptive to the controls. But is important to actually incorporate the feedback and implement the improved version of controls. Since this study collected cross sectional data, we did not get the opportunity of actually observing the new set of controls or policies being implemented based on the feedback received from the people. A summary of what CCIT is doing to improve monitoring and feedback is provided in table 5.12 below.

Table 5.12 Monitoring and Feedback at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Develop Monitoring and Feedback Channels	"The system in which I am right now, I am in a place where I am able to find out what they have done whatever needs to be done, seeing the audit trail. If they haven't done their work, we find that pretty quickly"	♦ Has tools for monitoring ♦ Sessions for obtaining feedbacks ♦ Feasibility analysis of the controls through monitoring

5.3.13 Achieving group cohesiveness at CCIT

Enhancing group cohesiveness helps in regulating the group behavior about security controls. Our data shows that peer pressure and groups' behavior influences and shapes the behavior of the individuals. The sub objectives under this are: encourage ability to share the work and credit for good work, discourage favoritism and self interest in groups and respect personal integrity in the group. Developing teams (Eloff and Eloff, 2005) is an important objective. People derive part of their identity from work groups (Hogg and Terry, 2000). The groups influence whether particular rules and controls would be followed or not. Thus encouraging cohesive groups with favorable security governance perception can help the organization's security program.

The management at CCIT believes that it is in the best interest of the organization to assign critical and vulnerable jobs to groups and not individuals. As observed by the manager, end user services:

> [We need to know] which roles have greatest vulnerability to assign groups. A great example of that is, if you multiple people together, collusion is lot harder compared to one person doing something wrong. So it's a similar type of thing, people in groups are afraid that others might know what they are doing. Groups have an impact on their behavior.

The management believes that it is easier to regulate and manage group behavior than individual's behavior. So if the groups are tight and cohesive, it would be beneficial to impart good knowledge about controls to the groups and expect the dynamics of the group to take care of the conformity part. The management also encourages the groups to achieve goals. The groups' achievements could actually trickle down to the individuals. As explained by enterprise systems team lead:

> What can you say at the end of the day that you have contributed? Ideally, you want the employees to plan in the beginning of the day; what they can accomplish that day, what is the next thing that they can do to accomplish their goals and then achieve something at the end of the day. Here is what I started out to do and here's what I did in the day, goals and accomplish on daily, weekly, and monthly basis in the way it's measurable. So control would be to motivate them as a group. Groups have a profound impact on the individual behavior.

The management at CCIT seems to follow this ideology to the core. There is evidence in research that suggests that individual behavior is influenced by the group that they belong to. Henry (2004) argues that conscientious and diligent employees can become the strongest link in an organization's information security infrastructure.

It was also evident from informal meetings and observations that the organization really has strong 'group' culture. There are several informal groups in this organization and solidarity of the members towards the group is quite committed. Open discourses with several employees suggested towards the politics of groups in decision making at the City council level. The awareness and knowledge about the controls did seem to vary a lot from group to group in the organization. It is apparent that enhancing group cohesiveness would certainly have an impact on the controls knowledge and behavior in this organization. Security governance efforts require teams with representation from all functionalities in the organization. The challenge is to organize the work of this team, to clearly specify roles and responsibilities, to train and sensitize team members to the work to be done, and then to make sure that they are in fact doing the work that management has indicated (Wood, 2006). Thus enhancing group cohesiveness in the security teams allows a coherent interaction channel with the management. A team approach to information security is

absolutely necessary if an adequate level of information security is going to be achieved (Wood, 2006). Chau (2006) argues for security professionals in development team from the beginning of the project. Trust also helps in making the groups tighter. Mutual trust helps in developing a strong sense of team within the organization as employee satisfaction is greatly dependent on their relationship with top management (Fleming, 2007). Research in group dynamics suggests that personal issues in groups can cause more damage to the organization than having job related issues. In a study by Trimmer et al (2000), relationship conflict was found to be more seriously detrimental to team success than task conflict. However, a high level of team conflict resulting from either source negatively impacts a team's success. IT staffers often demonstrate a sense of belonging to the IT team, due to their common expertise and training. If the managers implement clan controls (Ouchi, 1979) self-interested behaviors can be reduced. A summary of how group cohesiveness is enhanced at CCIT is presented in table 5.13 below.

Table 5.13 Enhancing Group cohesiveness at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Enhance Group Cohesiveness	"What can you say at the end of the day that you have contributed? Ideally, you want the employees to plan in the beginning of the day; what they can accomplish that day, what is the next thing that they can do to accomplish their goals and then achieve something at the end of the day. Here is what I started out to do and here's what I did in the day, goals and accomplish on daily, weekly, and monthly basis in the way it's measurable. So control would be to motivate them as a group"	♦ Set group targets ♦ Encourage group activities ♦ Track the people based on their groups ♦ Educate groups about controls

5.3.14 How does CCIT ensure management commitment for security governance?

Management needs to actively participate in security governance initiatives by rewarding conformity with controls and encouraging values such as a dedication, determination, open

mindedness and truth. If management communicates effective governance as "top priority", the controls instituted are considered seriously by the employees. Our data suggests that management should assess damage to the organization, as well as individuals, from lack of controls and take appropriate measures to instill desire to meet expectations about controls. All stakeholders should be allowed to participate in controls development process and the management should ensure that the voices are reflected in the controls. Management at CCIT participates actively in ensuring that right controls are developed and implemented in the organization. The input from the upper management is crucial for the success of the controls. There is evidence in the literature that suggests the direct relationship between security initiatives success and management commitment. Successful deployment of information technology requires management commitment, a structured decision making process and a strategy based on understanding of the vision and architecture of the organization (Shupe and Behling, 2006). Security would fail without consistent support of the management (Wright, 2007). Regular meetings and briefings with the top management reminds the management of the ongoing nature of security governance. By their commitment, corporate managers help pave the way towards the information society (Savola et al., 2005). It is clear from the attitude of the executives at CCCIT that if the management has the power, resources and the willingness to make the security governance a success story, nothing can stop the governance initiatives from flying. As explained by team lead of operations:

> Taking inputs from people is important, managers and directors. Decide how they want a particular environment, the money and resources to be used and the controls. Employees want more flexibility but really don't know what they

> want. Employees are always asking- why do we need to do this when you incorporate their inputs. Better approach would be stick to the top and find out what the management really wants and work with your given constraints. Find out what is it that you can do with these resources.

The top management feels that it needs to involve the city council and directors from the board to ensure that security governance is effective at CCIT. In case of developing new security policies and the controls, the managers are hesitant to take unfinished product to the board of the directors because once a decision is refuted by the board, its takes forever to actually get the decision changed. As the chief security officer shared;

> It [new policies and controls] should not go from us directly to the top, there are chances that it will not be approved. We should make it right the first time before we actually implement it. We need everyone's [directors from other agencies] perspective. It seems most of the things fall through the crack because of this[not involving other agencies], things don't work that way.

The CIO of CCIT gets involved in the development process of the controls and the policies at every stage and demands weekly progress report. He is also willing to provide resources to aid the process. The CIO invites outside consultants to provide their view on the policies and had ordered expensive textbooks, from where the policies could actually be referred. The top management shares the view that it is their job to protect the organization from risks and exposure and everything else is designed around this fundamental job requirement. As the CIO shared:

> At the end of the day, everyday, what's my job? My job is to manage risks. I assess risks and I make my decisions based on that. If you look in that regard, the idea that you should have a control program almost becomes common sense. The whole idea of having an internal controls program is to minimize risks and exposure. That's really what we do everyday in everything that we do; that is what management does.

The management has separate security department and has designated security officers who look after the controls management issues. This in itself is an indication of the management's commitment towards information security governance. As explained by the director, internal audit:

> Security officer position is a very critical position in the organization. That position has a formal training to manage these controls. To establish and manage these controls, security auditors try to make sure that security officer is doing the work competently

The management has to be proactive and work towards changing the corporate culture, and the resulting employee behavior (Drennan, 1992). The management at CCIT is clearly involved with security controls initiatives which provide a lot of visibility to the controls program in the organization. But a lot of security governance decisions need an 'okay' stamp from the higher management at city council level. Selling some of the governance ideas to this diversified gathering of board of directors is not easy. It is the duty of the management, nonetheless to use all the knowledge avenues and come up with the right decision for the organization. Management should be concerned about creation, protection and distribution of knowledge in the organization as it is a sources of competitive advantage.

Since the current CIO is committed to the cause of effective security governance, it appears that many of the initiatives might actually get approved by the board. The future of the governance program at CCIT is contingent upon several factors which are beyond the control of the immediate management. The tenure of the CIO, the political clout of the CIO

with the directors higher up and the vision of the city mayor about these things greatly impact the organization. We also observed that the top managements' involvement at CCIT actually deters non compliance in the organization. Research literature supports this relationship between the management commitment and deterrence impact. Organizations with top management support lead to greater deterrent activities than ones with weaker support (Kankanhalli et al, 2003) and eventually to better overall security. A summary of the assessment of management commitment at CCIT is presented in the table 5.14 below.

Table 5.14 Management commitment at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Encourage Management Participation	"Taking inputs from people is important, managers and directors. Decide how they want a particular environment, the money and resources to be used and the controls. Employees want more flexibility but really don't know what they want. Employees are always asking- why do we need to do this when you incorporate their inputs. Better approach would be stick to the top and find out what the management really wants and work with your given constraints. Find out what is it that you can do with these resources."	♦ Upper management participates in group meetings ♦ Management seeks inputs from people ♦ Management ensures that only the perfect version of the policies and control is presented to the higher management as City level ♦ CIO is supportive and gets updated on weekly basis ♦ Management ensures resources for the new development of policies and controls

5.3.15 Standardization of controls at CCIT

Standardization of the controls helps in benchmarking the governance activities, such as design and implementation of controls and investment security governance activities, against other players in the industry. It is important though to clearly differentiate between what needs to be standardized versus things that are best left unique to the organization. Standardization provides opportunities for learning from others and avenues for growth. It

also helps organization gain acceptance internationally in the eyes of regulatory authorities or third party vendors.

The controls developed at CCIT need to be specific to the organization. Being a service delivery organization, CCIT needs to set clear standards for what is expected from them and what would be acceptable. Having an idea about acceptable services, controls need to be designed in a way that at least the threshold level of performance is achieved. To provide a basic level of service, CCIT requires standardization of the process and hence controls. As explained by manager, development functions:

> I guess one of the other things which is very important and lot of people don't do this, establish acceptance criteria. That means that you are going to determine what the controls will do and how everyone has to act, for it to work, and then to ensure that it does act. It has to be consistent.

The management develops its own set of controls and then strives to standardize the controls such that maximum benefits could be derived from it through improved coordination. As shared by manager infrastructure services:

> I think every bureau has their own method [of developing controls] and in many cases may be they don't need to be at the same point because they have different applications. They all have a different way to do it. So it's key, it's important that it probably should have some form of standardization. I mean they [employees] need to be trained so they understand it works and a standard process helps in this [training].

One way of standardizing the controls is to look at the available governance models in the industry. Organizations should exercise caution while implementing the available frameworks as most of these frameworks cannot be used "as it is" and need customization. Use of established standards has been criticized in literature. Standards contain hidden complexities and nuances which can overwhelm the risk mangers who implement them.

Also effective implementation of standards requires a great deal of expertise on part of the assessor regarding risk assessments probably requiring additional trainings for the staff at large in order to make good use of formal methodology. Standards also suffer the problem of subjectivity where every organization interprets it according to their convenience (Lichtenstein, 1996). There is little doubt that security standards are not being readily adopted amongst the business community (May, 2007). But it also sees the value of looking at such frameworks. As explained by the director of the internal audit at the city;

> Somebody needs to do this, make sure that those objectives are being met by the systems. Those things [governance frameworks] have come into existence by looking at the experiences of several people who have suffered breaches. So, it's kind of learning from someone else's experience. It is critical to look at the frameworks.

There are benefits of actually standardizing the controls benchmarked against the commonly accepted frameworks in the industry. Research literature suggests benefits of standardization process of the controls. Standards are one of the best methods for companies to develop a proactive strategy for information security (May, 2005). The benefits are manifold: helps in developing structured strategy for security, offers reassurance to outsiders' vendors and boost to organization's marketing potential. Research suggests the importance of defining baseline controls and standard builds for platforms, systems and applications. These baselines may be the common ground of all risk treatment processes or it is possible to develop specific baseline sets for platforms of different roles, based on the level of risk (Wilson, 2005). As suggested by DeMaio (2002),

a significant characteristic needed to develop e-Trust in the network economy is the standardization of processes, interfaces and technologies.

The management also feels that standardizing the controls increase the acceptance of the organizations processes amongst vendors and enhances its credibility in the eyes of the regulators. The standardization process also helps in meeting the compliance criteria and is seen positively by the external auditors. In the process of development of new controls, the organization has not looked at the available frameworks so far. It would not be surprising though if the internal auditing demands adherence to existing governance objectives which forces the management to comply. It remains to be seen though, if the organization puts a blanket approval to all the controls from any standard framework to be used in the organization or only controls of operational nature are copied and the strategic ones are developed inside. A summary of standardization of controls at CCIT is presented in table 5.15 below.

Table 5.15 Standardization of controls at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Encourage Standardization of Controls	" I guess one of the other things which is very important and lot of people don't do this, establish acceptance criteria. That means that you are going to determine what the controls will do and how everyone has to act, for it to work, and then to ensure that it does act. It has to be consistent"	♦ Consistent controls ♦ Refer to the industry frameworks ♦ Required for the theird party vendors

5.3.16 Alignment of individual and organizational values at CCIT

This objective implies that security controls should be in alignment with individual's beliefs and values such that the probability of success of governance program increases. This alignment could be achieved in so many ways. Respecting other people's opinion,

involving other stakeholders in the control development process and incorporating employees' perspective in control design are some of the ways to approach the alignment task.

The CCIT management is appreciative of the fact that employees need to play an important role in development and implementation of the controls. Leach (2003) argues that in situations of conflict between individual and organization value systems, most people are unable to survive the tension for long. Even in the light of various legislations the agency had to follow, there were incidents of non-conformity with rules and regulations. It is to be noted that in the recent past, two employees form the department were terminated for non compliance with Internet surfing policies. These employees visited web sites that were restricted for the department network. In a newspaper report (not cited for confidentiality reasons), one of them had mentioned that he did it because he thought it was okay once in a while. The rules and the laws can only provide a direction for accepted behavior. But unless the rules are in sync with the individual values, there is a higher probability that it would not be followed. As the chief information officer of the agency mentioned:

> So we can make a rule, we can make a law that you have to be honest. I mean, in reality, our personal values, our own values should define that we are going to do the best we can, do the right thing at any point of time. If my personal values allow then only I will follow the rules. My personal belief is that you can't legislate that; you can't provide enough legislation to do that.

The organization, as mentioned above, was in the process of development of security controls for the entire city agencies. Being the IT department for the City, all the controls developed and approved by this organization would be applicable and enforced on other

agencies under the City. This means representation from various quarters of various agencies which were not even working directly with this organization. This represents a unique situation for control development. The agency which is responsible for development and enforcement of the controls is not in touch with other agencies which need to comply with the controls. The security officers, in charge of leading the control development process, understood the complexities involved. The Chief Security Officer at CCIT explained:

> It's very complex [developing controls]. Reach out to HR, legal people, get all resources to learn from them. Draft things that can actually work for everyone. You need to take all stakeholders in confidence, win their trust and ensure that you are working for them [individuals] not against them. It is what they need.

The management at CCIT uses psychometric measures to influence people to think that the controls are about them and not about the top management in the organization. The CIO has developed mechanisms to informally bring the end users on board with the controls. The security team in the organization reaches out to the people in a way so that they find it appealing. It is common in this organization for the security people to have frequent lunches with other stakeholders in order to "draw them in". Sometimes the bosses higher up make it mandatory to attend the sessions about controls and policies. But the intention of the people responsible for the controls is to make it more appealing to the users. The controls are being portrayed as something that is important for the employees, to protect them from any damage or harm in case of a security breach or a natural disaster. It is also a vehicle that makes the daily work easier. The managers accepted though that it is hard to ensure that the users continue to listen to them.

The influence of environment on individual beliefs and attitudes is well documented in literature (Thomson and von Solms, 2008; Kilmann et al, 1985; Dhillon, 2001). Lack of alignment between individuals and the organization leads the employees to work against management expectations, miscommunications, lack of cooperation from employees and environment complacency (Sathe, 1983). A lack of alignment leads to user resistance about the controls. User resistance manifests itself in various ways, including improper use of the security mechanisms (Schultz et al., 2001). Systems with a poor usability design tend to evoke a greater degree of user resistance (Al-Ghatani and King, 1999) and employees exploit the vulnerability already present in the system. The management and the security team at CCIT are aware of the importance of incorporating individual inputs into the controls. The management clearly wants the controls to be incorporated well into the processes and takes extra efforts to explain to the users about significance of the controls in their lives. Getting security controls and polices approved in the City is a very tedious and political process that involves managers and directors from various other agencies. In an environment such as this, efforts for individual and organizational alignment can go only so far. But the recognition of the fact that individual values matter should be helpful in the long run for CCIT. The attempts of changing the attitude of executives about security controls and developing people oriented controls should help in better understanding of the controls. No matter what the extent of technical and formal controls, prevention of insider security breaches demands certain normative controls. Such controls essentially deal with values, belief system and culture for the individuals (Dhillon, 2001). Behavioral change is

ultimately the result of changes in beliefs (Dhillon, 2001). A summary of the initiatives to align individual and organizational values at CCIT is presented in table 5.16 below.

Table 5.16 Ensuring alignment of individual and organizational values at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Ensure Alignment of Individual and Organizational values	"Draft things that can actually work for everyone. You need to take all stakeholders in confidence, win their trust and ensure that you are working for them [individuals] not against them. It is what they need" "I mean, in reality, our personal values, our own values should define that we are going to do the best we can, do the right thing at any point of time. If my personal values allow then only I will follow the rules"	♦ Use psychological measures to understand employees ♦ Have frequent lunches to "draw in" the employees ♦ Portray controls as something to protect the employees against harm. Its about them not the bosses

5.3.17 Resource allocation for controls at CCIT

Resources are the lifeline of the security governance program. Before developing the right controls and implementation plan, organizations need to take initiatives to develop the right environment for controls. Some of the proactive control initiatives that this research suggests are getting adequate resources for developing physical controls, encouraging co-ordination between departments and discouraging an environment of fear and politics in the organization. A clear vision about security governance is required to start groundwork before establishing the controls infrastructure. The dividends of such actions a priori planning eventually help the security posture of the organization.

The biggest issue that emerged from the case study at CCIT is the concern of the management about lack of physical and environmental controls. The management was worried about inadequate protection of not only the physical assets in the form of computer

monitors, CPUs and printers but also the crucial information in garbage cans. As shared by the administrative head of the organization:

> The other issue which we have had is the physical security of assets by temporary workers. The cleaning people are not the city's employees, they are from a company. They are brought in as temporary workers and are managed by a city employee. They come in and they got a giant trash can with them. Actually we have lots of equipments lying around, it's not a lot of money but it is some money. They can take away anything they want. How can I control that? They got to get in and clean the trash. If someone puts all the papers in the trash can and take it away, I won't know.

The manager's concern did not seem unwarranted for. The protection measures of physical assets in the office complex seemed complacent and half hearted. For example, a general protocol for a visitor in the office area is to first sign in at the registration desk, get a batch and wait to be escorted by the person they are supposed to meet. The visitor is also entitled to be shown the way out to the reception after the meeting. It is a control put in place for restoring physical security of office space and assets. But the employees feel it is a ridiculous requirement to have. The argument being that several vendors visit the premises on a weekly basis for years and it is silly to go get them every time and escort them back. It takes the employees away from work. An important point to be noted is the furniture layout in the office area. All the employees at manager level have closed cubicles and directors have their own rooms. There are no open area work stations in the entire organization. But a lot of equipments such as printers, copiers, monitors, CPUs and mouse are lying around in open areas where everyone has a common access to it. The layout is such that, for the most part, you cannot watch the activities in the open area from a cubicle. The concern of the administration manager seems genuine since there is lot of equipments

and important papers (in the printers and copiers) lying around and anyone can walk away with these papers without getting noticed. As she puts it, “we haven’t got into lot of trouble yet because we have been lucky so far”. Some of the directors echoed the similar threat and shared their disappointment at not doing anything concrete about it.

Currently the administration manager is the warden of the floor at City Hall where CCIT is situated and she does not have access to any blueprint of the building with her. As she observed:

> It really upsets me. They have made me the floor warden; I don’t even know how to get into those nooks and corners of the floor. It costs money to develop reorganize things in an easily accessible manner. There is lot of complacency because of that.

The administration manager has no way of knowing, in case of an emergency, where are various people exit doors in the building and how to reach various corners of the office and check if anyone needs help. For the sake of emergency preparedness, City does store some wheel chairs and masks for the employees within the facility. But the administration manager made a mockery of this ill planned attempt of the management saying that she was the floor in-charge for emergency needs and even she had no clue about how the digital locks work where the emergency equipments are stored. To her knowledge, the locks were quite old and no body was quite sure how it actually works.

All the stakeholders at CCIT unanimously argue for more resources to be injected into security controls to take the security governance plans forward. In this state agency, the resources are allocated after deliberations through several layers. This delays the benefits of some of the measures. The organization requires resources in monetary form as well as

more personnel urgently. These resources are important for the governance program but are lacking nonetheless at CCIT. As shared by the security officer:

> You know I want to do encryption of certain things that helps me to be able to monitor. People send me ssn [social security number], credit card information and I want to protect that. We have tools you can buy and put them in place to protect that [data]. We don't currently have those; it's a great job to get those tools, to get the funding for that, to get the people for that.

The political environment at City headquarters gets the better of the CIO and many a times good security control initiatives do not produce intended result. The management at CCIT should understand that developing adequate security mechanisms is a process of trade-offs between high security, usability and cost (Savola, 2007). The adequate level of security has to lie in the intersection of these three planes. All stakeholders, such as managers, developers, security experts and end users, should be on board in making such tradeoff decisions (Savola, 2007). Security governance decisions require coordinated efforts from all levels of management. The management at CCIT should influence directors at the City level about priorities and resource allocation for security and early involvement of security specialist in new projects or initiatives. Research literature has evidences to suggest that such teams are helpful in getting the right resources. Appointment of an expert team to conduct the strategic planning and resources to carry it forward (Shupe and Behling, 2006) helps the cause of security governance. The case at CCIT establishes the resources as a vital requirement for effective security governance program.

Research literature in security governance suggests that physical access is one of the most important but neglected issue in security management (Schauer and Essex, 2001). And this

is what we observed at CCIT. Security governance program at CCIT realizes the need for resources for physical security measures. The result is a compromised security control structure that is vulnerable on several fronts and needs immediate attention. Organization's building and premises, equipment and information processing facilities must be fool proof to prevent unauthorized intrusions and access and possible theft issues (Parker, 1996). The risk of poor security should be articulated such that budget and resources allocation is not compromised (Wright, 2007). Extant literature suggests measures that CCIT could adopt to get proper resources. Management must discuss with personnel the appropriate actions to be taken in the case of unknown people entering the premises or leaving it (Schauer and Essex, 2001). Devices to lock computers can be installed (Schauer and Essex, 2001). Laptops security should be ensured when the user is away from office and the organization should have strong policies and about this. Keeping a watch regularly on trash habits includes printed reports, diskettes, hard drives and zip drives that are being discarded or given away (Schauer and Essex, 2001). Applying such measures could help CCIT deal with the pressing concern about physical and environmental controls. A summary of resources allocation efforts is presented in table 5.17 below.

Table 5.17 Maximizing resource allocation for controls at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Maximize resource allocation for controls	"Consistently they [employees] must learn to trust. When you say you are doing something it means you are doing it; when you say you will get back to them, you get back to them" **"**We have tools you can buy and put them in place to protect that [data]. We don't currently have those; it's a great job to get those tools, to get the funding for that, to get the people for that" "It is like buying auto insurance the day after you had an accident. It is not going to help you the damage is done already. So is the case with the security controls for the	♦ Enhance trust measures in the organization ♦ Seek more resources to get the controls working ♦ Registering at the front desk before entering the organization and at the time of departure ♦ Escorted by the employees into and out of the office

management. If you are not doing something to police it on your own then you are going to find about it after it really happens. So there is really nothing you can do, there is nothing you can do to protect yourself as you have already experienced the vulnerability"

5.3.18 Visible executive leadership accomplished?

Effective information systems security governance program requires visible leadership to provide the direction to controls management in the organization. This objective entails a leadership style and philosophy that provides the momentum to the controls program. The perception about security governance is created by the leaders who should be able to "walk the talk". This objective demands that the leadership in that organization should present exemplary behavior and be able to nurture relationships with cohorts. Promoting executives with good security governance understandings in visible leadership roles should be an integral part of the governance program.

The security managers at CCIT have faith in their leader i.e. the CIO of the organization. But the other factions of the top management at the City are ignorant about the needs of the security program and have little interest in knowing what's best for the organization. As explained by the security manger:

> With the city, it's not hard to get the support of the CIO. He is supportive of our actions. The hard part is getting to his colleagues, the other directors, who need to approve it but have no clue about it.

The lack of support from the leadership is hurting the new security governance program at the City. The general perception is that if the CIO is supporting the cause of the security controls, the program would be in effect sooner or later. The vision and dedication of the current CIO has actually been crucial in developing new security initiatives at CCIT. As

suggested by the objective, managers in this organization believe that leaders should be able to set an example for the rest of them to follow (see table 5.18). No control program can work if the leadership in the organization conveys contradictory message about the intent of the controls. Research literature in information security area calls for consistency in leadership about security issues. The executive leadership should espouse that controls are important and be consistent in behavior to convey what is espoused is real (Drennan, 1992). Senior managers can communicate policies and codes of ethics to guide employees (Krull, 1996). It is the responsibility of the leaders to serve as a role model for the behavior it wishes to promote (Krull, 1996). Executive leadership sets the tone for employee trust as the core for company's success and is reflective of the culture in the organization (Fleming, 2007). If a control is being endorsed by the executives in the top management positions, it is important that the control is followed. As explained by application services manager:

> A very good example here is that in an organization you tell people, if you share your password and this is the law, you will be fired. Then president of the company, she goes to some other site and shares her password with others. You need to make sure that if you set something up, you need to set an example for others to follow and then you can control the process.

In the light of the above objective, the organization is actually undergoing great changes in security governance program under capable leadership of the current CIO. The head of the organization has great understanding of the security issues and is willing to instill good values about security governance at CCIT. It is a part of the governance duties of the executive management to encourage employees to adhere to the behavior expected to

contribute towards the successful protection of information assets (Thompson and von Solms, 2008). Visible management is required to actually employees at all levels really internalize the code of conduct they want employees to follow. Leadership also leads to trust building and ethical environment in the organization when employees see consistency in behaviors. But being a part of the bigger organization (the City), CCIT does suffer temporary setbacks in their security governance program due to non cooperative directors and their lack of knowledge about security issues. Visible leadership plays a decisive role in every security initiative planned by the organization. a summary of leadership initiatives at CCIT is presented in table 8.18 below.

Table 5.18 Visible executive leadership at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Establish Visible executive Leadership	"With the city, it's not hard to get the support of the CIO. He is supportive of our actions. The hard part is getting to his colleagues, the other directors, who need to approve it but have no clue about it"	♦ CIO is supportive of the new security policies and controls ♦ Take into confidence the leadership at the city level

5.3.19 Ethical and moral values instituted at CCIT

This objective suggests development of appropriate ethical environment for information security governance. An ethical organization would encourage right work ethics and institute appropriate moral values in the employees to shape a favorable perception about security controls. Management should encourage people taking pride in their jobs and that right display of morality is rewarded and valued in the organization. A strong leadership helps in actually establishing the importance of ethics and morality in the organization. At CCIT, management believes that ethical and moral values as something integral to the employees and there is not much that can be done to change it. Research literature supports

this assertion. In a study about impact of general and IS specific codes of ethics on computer abuse intentions, general codes had no impact of users intentions while IS specific codes ethics has a slight effect on one type of computer abuse (computer sabotage). Organization can have a code of conduct as documenting its ethical values but it is difficult to assess the operating effectiveness of such a control (Ramos, 2005). Management has to evaluate the effectiveness of such a code (Ramos, 2005). At CCIT, the director gave an example of regulatory compliance issues in the organization. Even though regulations are meant to ensure that people do the right thing, it really does not help organizations in this direction. The director said:

> so we can make a rule, we can make a law that you have to be honest. I mean, in reality, our personal values, our own values should define that we are going to do the best we can, do the right thing at any point of time. If my personal values allow then only I will follow the rules. My personal belief is that you can't legislate that, you can't provide enough legislation to do that

The management at CCIT believes though that if the leaders "walk the talks", they can certainly be exemplary in the organization and thus set an ethical and moral standard to be followed by the employees. The CIO of the organization is one such leader who is "looked up to" by the employees in general. The management respects personal integrity of people and rewards examples of the ethical and moral behavior through a "star of the month" program. In this program, employees who have in some way set examples of good ethical behavior, which can influence people, are acknowledged publicly by the management monthly and the description of the behavior along with the winner's name is displayed in the meeting areas. This has actually influenced people positively and communicated a

message from the management that ethicality and morality are important and these qualities are valued in the organization. There are evidences in literature to support the management's belief that it can influence the ethical and moral environment in the organization. Information Systems professionals generally demonstrate a solid understanding of information security ethics as they apply to organizational goals. Dhillon and Torkzadeh (2006) suggest that instilling value based work ethics would help in ensuring an ethical environment which leads to employees' deterring from unacceptable behavior for a secure organization. The security governance initiatives must supplement the old technical and procedural mix of controls with the ones aimed at morality of the insiders. The security technology design often neglects the moral or ethical element of the governance process which is one of the most important aspects of security management (Gupta and Sharman, 2008). Addressing this pertinent issue, Gupta and Sharman (2008) suggest a model that offer insights into social behaviors that unravel the risk exposure of the organization from social engineering attacks. The authors develop a social engineering susceptibility index (SESI) that uses social network theory and organizational dynamics. Krull (1996) argues that employers must create an environment that encourages employees to recognize and respond appropriately. Standards and codes of ethics must also become part of the organizational culture and reward system. Whistle blowing can be encouraged by establishing policies that define appropriate responses to perceived problems (Krull, 1996). We observed that top management at CCIT works towards creating an ethical and moral environment. A summary of initiatives to ensure ethical and moral values in CCIT is presented below in table 5.19.

Table 5.19 ethical and moral environment at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Ensure ethical and moral values	"so we can make a rule, we can make a law that you have to be honest. I mean, in reality, our personal values, our own values should define that we are going to do the best we can, do the right thing at any point of time. my if my personal values allow then only	♦ "star of the month" program ♦ Leadership is encouraged to "walk the talk" ♦ Management provides the right environment

5.3.20 On trust building mechanisms at CCIT

The objective emphasizes the importance of role of trust in success of security controls in organizations. Building trust is important to ensure that individuals can work according the expectations of the management without close supervision. Trust is the enabling of confidence that something will or will not occur in a predictable or promised manner. The enabling of confidence is supported by identification, authentication, accountability, authorization, and availability. A positive environment where the leadership is dependable and the management less politicized, helps employees to trust the intentions of supervisors and each other for the best for the company. Employee beliefs about strong security governance in the organization are a good predictor of security success in the organization (Stanton et al, 2004). Outsider stakeholders should be able to trust the security measures in the organization to work with it and develop a positive perception about the reliability of the firm in the market.

The management at CCIT believes in trusting employees about day to day activities (see table 5.20). This is evidenced from the fact that there are a lot of equipments lying around in the organization without being locked. These equipments are not stolen and the employees believe that no body is going to take the City's property. Self-control can be

helpful in this environment (Kirsch, 1996). One of the mechanisms to build trust within the organization, as employed by the management, is to maintain consistency in behavior. As explained by the security director:

> They [employees] must learn to trust. When you say you are doing something, [make sure] you are doing it. When you say you will get back to them, you get back to them. You got to have that consistency.

The data suggests that trust is perceived as pivotal in the success of the controls at CCIT. The director of project management is of the view that trust needs to be cultivated on a daily basis with the co workers by respecting their points of view and engaging them in the decision process. As observed by manager project management:

> Consistently they [employees] must learn to trust. When you say you are doing something it means you are doing it; when you say you will get back to them, you get back to them. You got to have that consistency and managing controls is going to be the same thing, here is the policy, procedure, you must do it and it will be done.

Trust is an indicator of series of direct relationship with people and not with a series of organizational entities or policies (Fleming, 2007). This is evidenced in CCIT's trust relationship with other agencies under the purview of the City. There have been a number of incidents about the policies and the controls being developed at the CCIT being rejected by the council. As mentioned by the application development manager:

> I am talking about the whole city. They [other agencies under the City] have to trust IT to develop these policies and controls. We have best interest in doing so. It is good for compliance as well with any federal state and local law.

Other agencies and its directors are at loggerheads with CCIT top management about the content of the policies. The other directors at city council are afraid that these policies

would provide excessive power to CCIT over the other agencies with the City. Several board meetings and drafts later, CCIT is still struggling to get the policies okayed. The need for inter-organization trust building mechanisms is obvious at the City office. Research literature can guide CCIT in this situation of lack of trust with partners in business. Companies should be able to guarantee its trading partners that they enjoy a minimum level of acceptable security and have a certificate to prove that. This leads to trust building between trading partners (Trompeter and Eloff, 2001). CCIT could also try a novel concept that will enable information security professionals to implement effective security is 'e-Trust' (DeMaio, 2002). Inter-organizational business requires standardization of processes, interfaces and technologies that help in development of mutual trust in collaborating partners in business (DeMaio, 2002). Other agencies could use pre established criteria to assess what CCIT proposes. Organizations could use performance evaluation criteria that emphasize trust, security and control requirements (DeMaio, 2002). Research suggests that lack of trust in policies and monitoring systems can make the employees alter systems and simply not complying with controls such as not sharing passwords or taking confidential data out of the office on laptops (Booker and kitchens, 2008). This is what we observed at CCIT. Lack of trust impedes the optimal functioning of organization, as conveyed by one of the incidents shared with us. In one of the disaster situation, the organization sent a laptop to affected site for resuming normal functioning. Since the manager had to sign the receipt of the equipment and be responsible for it, she walked away with the equipment as she did not trust anyone to deal with it appropriately. The manager in question took it with her on a vacation; meanwhile, all the work that could

have been done could not be accomplished. This certainly shows how the spirit of the controls s defeated due to lack of trust amongst groups and mangers. On the other hand, there needs to be a caution in establishing trust with outsiders as it could be exploited for social engineering attacks (Gupta and Sharman, 2008). A summary of trust building mechanisms at CCIt is presented in the table 5.20

Table 5.20 Trust building mechanisms at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Maximize trust building mechanisms	"I am talking about the whole city. They [other agencies under the City] have to trust IT to develop these policies and controls. We have best interest in doing so. It is good for compliance as well with any federal state and local law".	♦ Equipments are lying openly in the office as there is mutual trust about not stealing City's property ♦ Managers maintain consistency in "saying and doing"

5.3.21 Ensure punitive structures at CCIT

Punitive structures require the management to establish clear consequences for non compliance with policies and ensure disciplinary action against unacceptable behavior. The impact of deterrence activities, according to our data, is significant for impeding non compliance with controls and policies. Deterrence helps in creating fear of punishments. It is important to explain clearly the meaning of criminal actions and in cases of non compliance, it is critical to take quick and responsive actions. Developing countermeasures helps in conformity with rules and regulations. Information systems security research has established the importance of deterrence criteria for better security (Dhillon and Torkzadeh, 2006; Straub and Nance, 1990, Straub, 1990). Researchers in information security governance domain have undermined the importance of deterrence activities and have practically not explored work in this area.

The management at CCIT, especially the CIO, is clear about establishing clear deterrence criteria as preventive measures for information systems security governance. As observed by the CIO;

> I also think what you have to do is to have a clear punitive structure because big things are at stake. A punitive structure is a must. So you must have some type of thing that says even if the employee violates this, what is going to happen to him.

A punitive structure constantly reminds the employees about the consequences of their actions. There are evidences from research to suggest that punitive structures actually deter employees from non compliance with policies. For instance, Darcy and Hovav (2007) empirically examined user awareness of security policies, security-awareness programs, computer monitoring, and preventive security software and their effect on user intentions regarding IS misuse. Their results suggest that a combined proactive and preventive approach to security deters users from IS misuse (Darcy and Hovav, 2007). Repeated efforts are required to instill the results of non conformity with polices into the minds of the employees. As shared by security manager;

> It is very important to establish consequences and give constant reminders. We have to go there again and again. What constitutes a violation? What are different levels of violations? Establish the penalties, the parameters of what constitutes non conformity. Nothing can be done later if you do this and if something happens do take some action

The top management also feels that one of the biggest drivers for establishing deterrence in not adhering to the controls in the organization is frequent auditing. The management believes that the process of auditing implies that "you are being watched" and "you will get caught" if you are deviating from the accepted behavior. This constant reminder

actually helps in deterring the employees form risk behavior and encourages respect for the controls.

Since the organization has fewer audits that it actually thinks it needs, the impact that this complacency has on deterrence is unpredictable. If people think that the audit is not going to take place, say for next three years, they actually might get tempted to break the law more often. If the employees think that there is no way of getting caught for the next three years, the behavior might be modified accordingly. This could actually have serious implications for the security governance in organizations.

Research in information security suggests several measures that could be adopted by CCIT to deter employees from deviant behavior. For example, the management could study employees' compliance and resistance behaviors and identify the most vulnerable areas which are not easy to be policed. This helps in creating deterring activities aligned with the employees' tolerance towards such measures (Booker and Kitchens, 2008). CCIT could use more deterrence efforts to develop a preventive security management approach. Kankanhalli et al. (2003) argue that greater organizational deterrent efforts (in the form of person-hours expended on IS security purposes) and preventative efforts (in the form of more advanced security software) were associated with higher perceived IS security effectiveness. security countermeasures that include deterrent administrative procedures and preventive security software results in lower computer abuse (Straub, 1990). For maximizing deviant behavior, CCIT could reinforce positive beliefs and attitudes, in other words first clarify what behavior is unacceptable through clearly establishing the ethics and

morality expected from the staff. A summary of establishing a punitive structure in organization is presented in table 5.21 below.

Table 5.21 punitive structure at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Ensure punitive structures	"I also think what you have to do is to have a clear punitive structure because big things are at stake. A punitive structure is a must. So you must have some type of thing that says even if the employee violates this, what is going to happen to him."	♦ Explain consequences and send reminders ♦ Clear punitive structure ♦ Punish in case of security breach or non conformity with controls

5.3.22 Training and education about controls at CCIT

Education about need for controls creates awareness in the organization about risks, responsibilities and social engineering issues. Training employees about usage and scope of controls helps the end users in understating the impact of controls on day-to-day work and also reminds people to apply their knowledge in practice. Training should be enforced and the impact of such measures should be assessed periodically. Our data establishes the importance of training with specific focus and work related examples. Regular training programs should be designed early on in the security governance strategy.

Training and education is greatly emphasized in CCIT, in theory and in practice. The upper management in the organization schedule regular training of the employees on various issues including security awareness and controls. The belief in training and education is echoed by a security officer:

> You can put control such as discussing the policies. But in my opinion controls are not going to do anything unless you educate your end user. Understand that controls don't do anything for you unless you educate end users.

The management has a preventive approach towards security management and invests in protecting the organization and the employees proactively from vulnerabilities. Training the employees on use of various applications for business processes and other related technologies ensures a better understanding of the expectations from the employees. The management is proactive about providing enough information to employees about policies and control and is perseverant about making sure that the employees actually read the material are aware of its contents. As shared by chief security officer;

> Human nature it is that they [employees] may read the policy and go "ok I do know that" but they wouldn't read in the details. There is an education factor also, to get the word out to people. When you sign these forms, this is what it meant and you are held responsible. Part of the procedure and guideline will hold, make it standard this is what happens when you don't do this, first warning, second warning, third warning. I believe that our HR is working on some of that now [chief security officer]

The management takes extra measures to ensure that the education is actually reaching the end user and provides extra incentive so that the material is read and understood y the user. As the administrative manager commented:

> Education and reaching out to the employees [is important]. Reward them [employees] for reading and knowing the controls. Give a gift certificate. If you do this, take this test after reading and pass, you can go for this incentive. Typically if you make it mandatory, they [employees] go and find it because they have to go and look. Make it appealing to the employees, .explain that it helps me in my normal everyday life and not because it is a burden or something that needs to be done to survive.

The training and education emphasis at CCIT has been helpful in creating awareness about security controls and governance. There is evidence in research literature to support CCIT's efforts on training and education. The success of IS security depends largely on

end-user behavior and awareness (Darcy and Hovav, 2007). Defining ways to inform and educate users on what constitutes legitimate use of IS resources training involves alerting users to known vulnerabilities and threats and through preventive security technologies (Darcy and Hovav, 2007). Fuller et al (2007) conducted a study to examine the impact of training on information assurance awareness and knowledge retention in the organization. The results suggest that employee information assurance knowledge erodes over time suggesting a need for recurring training.

The management utilizes resources for the knowledge of its employees about security control issues which in turn prevents the unintentional breaches of security. Training could communicate higher level concepts such as security action cycle but also detailed information about specific vulnerabilities. End users need to be educated on risk factors and how it affects bottom line (Garigue and Stefaniu, 2003). They should also be aware of emerging technologies and threats and business impact of potential security incidents. Extensive training is required to make the standards a part of organizational controls culture (Krull, 1996). The employees on the other had did not seem too happy with the training programs. It seems that the people who actually got the training did not see much value in the exercise. The importance of the training for the employees needs to be communicated clearly. It should not be a checkbox exercise which is to be done. The management's efforts of explain the employees "what's in it for me" does not seem adequate. This emphasis needs to be changed when the new controls program in instituted. A summary of training and education initiatives at CCIT is presented in table 5.22 below.

Table 5.22 Training and education at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Encourage Training and Education	"Human nature it is that they [employees] may read the policy and go "ok I do know that" but they wouldn't read in the details. There is an education factor also, to get the word out to people. When you sign these forms, this is what it meant and you are held responsible. Part of the procedure and guideline will hold, make it standard this is what happens when you don't do this, first warning, second warning, third warning. I believe that our HR is working on some of that now".	♦ Extensive training about applications and business processes ♦ Explain with work related examples ♦ Encourage use of knowledge in work ♦ Provides incentives for education (gift cards)

5.3.23 Clarity in business processes at CCIT

Establishing clarity in business processes is absolutely essential to maintain business integrity. This objective emphasizes the role of adequate understanding of the work flow and the coordination that is required for smooth operating environment. Unless the interrelationships of the business activities and the flow of information are clearly established, it is difficult to integrate appropriate security controls seamlessly and protect the business. Many businesses suffer vulnerability because of the lack of a deep understanding of the business processes resulting in inappropriate controls being implemented.

At CCIT, the management believes that controls should be integrated in the business processes and build along in a way that there would be no flow of processes if controls are not executed. For governance purposes, it is crucial to understand the business system and dynamics of business processes within the systems for good security (Savola et al., 2007). Especially it is important to recognize linkages of information security with business processes and have abilities to create and distribute new knowledge horizontally and

vertically in organization by using normal business interactions (Savola et al., 2007). The right measure of the importance of an imbedded control is that you cannot do your business if you surpass the controls. As mentioned by project management manager:

> Internal control means that you are following the right process, the right vigor, to deliver what the business wants. What does that mean? It means that you have to start in a clear, precise way about the scope of what you want. Clearly define the requirements and then you get everybody who is involved to agree on those [requirements] and then from there, you build out your processes.

The controls should be aimed at improving the business efficiency. The provision of clear insight and advice in terms of IT strategy ultimately contributes towards an improved system of internal control that better supports the organization's overall corporate governance objectives (Myler and Broadbent, 2006). The general sentiment of the management regarding controls is that it should be planned way ahead and instituted in the processes proactively and not as an afterthought (see table 5.23). The common belief of the management was echoed by, security manager:

> I think they [controls] should be designed to help to ensure that your data and processes are sound, that your money is accounted for and your resources are applied correctly. Also, your performances and expectations are met as an agency. It should basically improve the business process.

There is again an apparent contradiction about what the management believes and what it does. At CCIT, the business processes are institutionalized and controls are always added as an afterthought. Service delivery being the prime business of the organization, it is important to ensure that data is accurate before providing it to the customer. A summary of efforts to achieve clarity in business processes is presented in table 5.23 below.

Table 5.23 Clarity in business processes at CCIT

Objective Name	Evidence from CCIT	Measures at CCIT
Establish Clarity in Business Processes	"I think they [controls] should be designed to help to ensure that your data and processes are sound, that your money is accounted for and your resources are applied correctly. Also, your performances and expectations are met as an agency. It should basically improve the business process".	♦ Control the software purchasing system ♦ Controls build along the business process ♦ If controls are not executed, cannot run the business

5.4 Relevance of ISG objectives at CCIT

The management at CCIT identifies security governance as a strategic driver for ensuring effective service delivery to the other agencies under the City. The organization is in the process of redefining its security governance program. The desired changes in the security governance objectives in the new program are reflective of the managements' dedication to develop a critical IT infrastructure free from vulnerabilities. The proposed ISG objectives were discussed at length with the representatives from the top level, middle level and operational management in the organization. Depending on the nature of their roles, respondents from each level of the management identified with different types of objectives. The interaction with CCIT offers three different perspectives on the use and importance of the developed objectives. Each of these perspectives is discussed below and a synthesis is presented in conclusion of the section.

5.4.1 The top management perspectives on ISG objectives

The top management is responsible for the defining the strategic direction, providing leadership and resources for the security governance program. The CIO and the directors at CCIT could identify better with the objectives with leadership and strategic aspects of security governance. The objectives, *Maximize resource allocation for controls, Ensure corporate controls strategy* and *Ensure visible executive leadership* emerged as really

important for the top management at CCIT. By definition, the role of the top management is about strategizing and allocating resources for security purposes (Ansoff, 1985). The objectives *Ensure punitive structures, Ensure formal controls assessment functionality, Maximize management commitment and Ensure ethical and moral values* were rated as important for the success of the security governance program.

The top management at CCIT believes in commitment to security governance initiatives and consequences of non compliance are very important for the success governance program. Establishing separate controls assessment functionality could only help the cause of strong controls in the organization. As explained by the chief security officer:

> He [CIO] is supportive of our actions. The hard part is getting to his colleagues, the other directors, who need to approve it but have no clue about it. But we depend on the CIO to get the things done. He helps in getting them [other directors in the city council] on board.

The top management perspective about security governance at CCIT is about emphasizing the importance of resource allocation for making sense of the controls program. This perspective emphasizes the importance of resource allocation in attaining a feasible security governance program. Resources in the form of finances, people and technology are essential for effective security governance. As one audit officer pointed out:

> A strategy for good governance is good, but we do need the resources, may it be in the form of money, people or infrastructure.

The extant research literature in this area recognizes the importance of the objectives important to the top management at CCIT. The need for controls strategy has been articulated in the research literature even though not explicitly. In the literature, there have

been explicit calls that information security should be integrated into an organization's overall management plan (Perry, 1982; Lane, 1985, Smith, 1989).

Perry (1982) argues that computer security and control strategy establishes a climate and need for control. Since strategy is such an integral part of control design, it must be understood and formulated prior to designing the controls. Organizational strategy establishes the managements' intent, concern and means to achieve the control objectives (Perry, 1982). Management needs to convey the expectations about the controls to the employees. Thompson and von Solms (2008) argue that it is a part of the governance duties of the executive management to encourage employees to adhere to the behavior expected to contribute towards the successful protection of information assets. The executive leadership should espouse that controls are important and be consistent in behavior to convey what is espoused is real (Drennan, 1992). This should ultimately lead to the shared tacit assumptions of employees becoming aligned with these espoused values of the organization, thus progressing towards an Information Security Obedient Culture (Thomson and von Solms, 2008). The management has to be proactive and work towards changing the corporate culture, and the resulting employee behavior (Drennan, 1992). This leads to establishing punitive structures which allow policing and safeguarding organizational resources within the organization.

5.4.2 The middle management perspective on ISG objectives

Establishing process integrity through efficient auditing practices, standardization efforts and superior technical competencies come together as key aspects of information security governance for the middle level managers at CCIT. The middle management perspective is in emphasizing the due process in achieving process integrity for information security governance. The objectives that emerged as the important ones to the middle level managers at CCIT are *Ensure Efficacy of Audit Processes, Ensure data criticality and clarity in control development process.* The middle level managers believe that audit

should be done frequently. The control development process should have clarity and data criticality should be strived for through adequate access controls and authorization mechanisms. As senior audit manager explained:

> If you don't understand that HR may be the one place you go. I [an employee] don't understand what it [polices and procedures] means, ask this upfront. Having to own the policies, it [the management] should be responsible for the procedure for this procedure, be responsible for answering those questions. Clarifying the concepts helps people in believe in the governance program in the management.

Also, the objectives *Encourage Standardization of Controls and Maximize trust building mechanisms* were deemed significantly important by this group of people. The middle level managers strived for developing benchmarking standards in controls development. The managers also believed that trust within the organization and with the stakeholders outside the organization is crucial for the success of the security governance program. Research literature acknowledges the importance of the objectives identified by the middle level mangers at CCIT. Data criticality is important and if organizations do not ensure that all employees understand their information security roles and responsibilities, it may become difficult to protect the confidentiality, integrity and availability of information assets (NIST Special Publication 800-16, 1998, p 12). For governance purposes, it is crucial to understand the business system and dynamics of business processes within the systems for good security (Savola et al., 2007). Especially it is important to recognize linkages of information security with business processes and have abilities to create and distribute new knowledge horizontally and vertically in organizations by using normal business interactions (Savola et al., 2007). This perspective of ISG acknowledges

importance of developing and maintaining process integrity for security governance. Management should be concerned about creation, protection and distribution of knowledge in the organization as it is a sources of competitive advantage (von Krogh, 1998). This allows a controls strategy to fit into the overall organizational strategy for business growth and security is viewed as a strategic governance issue (Lane, 1985, Smith, 1989). All the above measures require trusting people in organization to do the right thing at the right time in the right way. Trust measures work within the organization to coordinate and improves the controls initiatives and outside the organization to enhance the perception about security governance efforts of the management.

5.4.3 The operational management perspectives on ISG objectives

The operational management respondents comprise security officers, auditing officers and help desk people. The operational people are the ones who are actually responsible for the operational efficiency of the business. The staff works with the controls on daily basis, yet their representation in the development process of the control is minimal. This group of respondents identified themselves with the objectives that emphasized the importance of individual user involvement in the success of security governance. There was a unanimous agreement in the group about the importance of having a control conscious culture in the organization. The operational people felt that the culture would guide them in times of confusion.

The objective *Maximize clarity in business processes* was considered very important by this group. This is because the objective directly impacts their domain knowledge expertise and work. Clarity in business processes is crucial to develop controls that do not allow

vulnerabilities to seep in the business. *Ensure Communication about Controls* objective advocates well established communication policies about open discussions on controls between the management and the employees. Communicating was considered crucial by the operational people since it is really important for them to clearly understand the scope and intent of the controls. *Maximize monitoring and feedback* objective is also crucial for this group as it provides an opportunity to actually change the controls that hinder the work process. The objective *Maximize Group Cohesiveness* was rated as very important by this group. The respondents felt that peer pressure and behavior of other group members played an important role in the acceptance of the controls. *Ensure Alignment of Individual and Organizational Values* signifies the importance of individuals' value system aligned with the management's philosophy and organizational values. The respondents felt it is really important to understand if the organizational values are in line with their personal value system. The objective *Maximize Training and Education* implies continuous training and education of the end users and members of the operational group felt that unless adequate training is provided to them about the controls, no governance initiative will sustain in the long run. As mentioned by a security officer:

> They [users] need to be educated about the initial controls as well as the reasons for change. Communicate clearly and effectively about the changes in controls because things change, business needs change and so do controls. Business processes should be well understood for this.

The operational management people could identify more with the objectives that represent an underlying theme of the importance of individual participation for the success of security governance. This conjecture is supported by the research in information security

governance area. Conscientious and diligent employees can become the strongest link in an organization's information security infrastructure (Henry, 2004). Pointing out the importance of individual participation in governance efforts, Thomson and von Solms (2008) argue that the environment within the organization has the most influence on employees' beliefs and attitudes. If there is a misalignment between individual and organizational values, the employees might move in the wrong direction and against the expectation of the management (Kilmann et al, 1985). Such an environment can be detrimental to security governance in the organization and may lead to miscommunication, lack of cooperation from the employees and complacency in performance (Sathe, 1983).

5.4.4 What do the perspectives mean for information security governance?

The three perspectives at CCIT suggest three emergent dimensions of information security governance: user involvement, process integrity and resource allocation. A synthesis of the three perspectives suggests the relevance of all the proposed objectives for CCIT. The emergent perspectives are the conceptualizations about security governance that is reflective of the nature of the work an individual does and the kind of organization she belongs to. The perspectives from three levels of management are not something unique to CCIT. Research literature in management and information systems suggest three dimensions of managerial decision making. Weill and Ross (2004) and Peterson (2004) suggest similar dimensions or perspectives in organizational governance for information technology. The authors claim that actions of decision makers across business units in the organization requires three coordination mechanisms namely process based, structural and relational. Process-based mechanisms are the formalization and institutionalization of

strategic IT decision making or IT monitoring procedures (Peterson, 2004). This dimension is similar to the middle level managers' perspective about the importance of process integrity for security governance at CCIT.

The structural mechanisms are formal positions, roles, teams, and committees established to coordinate decision making in business and IT (Peterson, 2004). This dimension is similar to the top level management perspective about strategy and resources at CCIT. It is not surprising that the development of controls strategy and allocating resources for controls emerged as most important objectives for the top management. The relational mechanisms foster voluntary and collaborative relationships among corporate executives, IT management, and business management (Peterson, 2004) to help in clarifying differences and find creative solutions to problems. Self-control can be helpful in this environment (Kirsch, 1996). IT staffers often demonstrate a sense of "belonging to the IT team" because of their common expertise and training. If the managers implement clan controls (Ouchi, 1979) self-interested behaviors can be reduced. This dimension is similar to the operational level managers' perspective about importance of individual in the success of controls.

The dimensions proposed by Weil and Ross (2004) are in the context of effective IT governance in an organization. Being a subset of the overall IT governance in the organization, information security governance domain can theoretically extend the concepts. All of the three perspectives need to be integrated for designing comprehensive security governance at CCIT. All the objectives fall into one or more of these perspectives and are extremely relevant for the organization. A security governance program needs to

be designed along the lines of these underlying objectives such that the benefits from such a program are maximized. Based on the discussion about the emergent themes from the three perspectives, the relationship between the dimensions is shown in the figure 5.2 below.

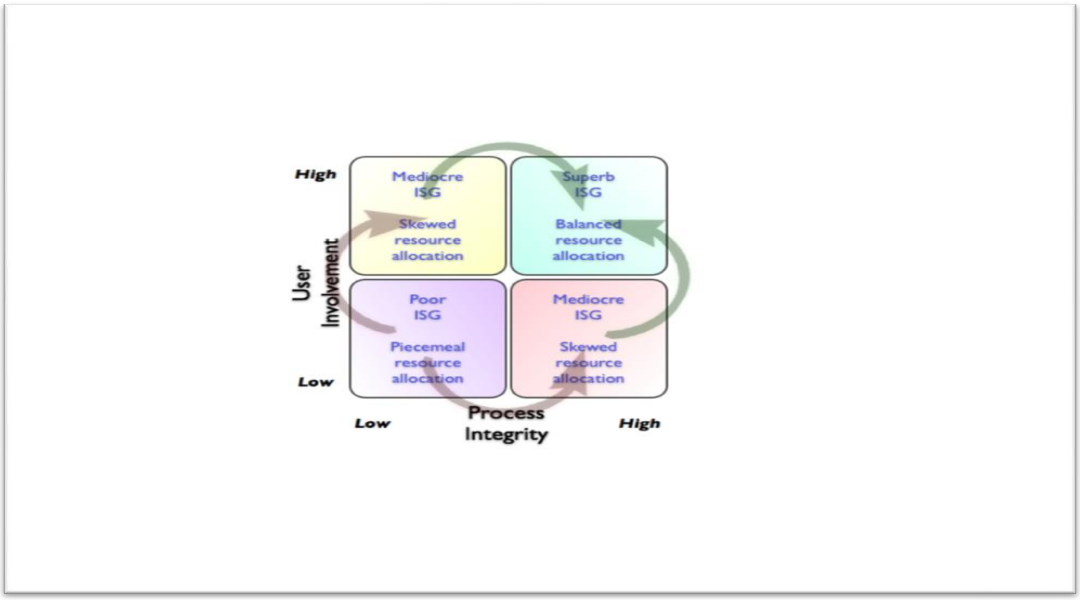

Figure 5.2 The User-Process-Resource (UPR) matrix for information security governance

The proposed User-Resource-Process (UPR) matrix shows the interdependence of the three dimensions of ISG. In the above matrix, the intersection of the two dimensions, user involvement and process integrity results in four stages of ISG, dependent on the resource allocation dimension. The lower quadrant on left side represents low process integrity and low user involvement with piecemeal resource allocation for controls. The result is poor ISG practices for organizations in this quadrant. Moving away from this quadrant in the clockwise or anti-clockwise direction (it would be very difficult to move directly in the diagonally opposite quadrant) and organization can either increase process integrity or user involvement. The resources allocation in these quadrants would be skewed in either

direction (depending on which quadrant the organization is) resulting in mediocre ISG practices. For example, if an organization is in the top left quadrant, in here the resources are skewed towards more user involvement and less process integrity initiatives. Similarly, if an organization is in the bottom quadrant at right, the resources are skewed towards increasing process integrity and user involvement is neglected. To reach in the ideal state i.e. the quadrant at top on right, where there is high user involvement and high process integrity requires balanced resource allocation for both the dimensions. Organizations in this quadrant would have superb ISG practices and this is the desired state to be in. This matrix explicitly establishes the relationships between user involvement, process integrity and resource allocation for maximizing ISG in an organization.

5.5 Discussion

In phase two of the research, the data from CCIT clearly establishes the importance of all the information systems security governance objectives developed in phase one. The objectives are considered important by the organization and each and every objective, to some extent, is being realized by the management through various measures at different levels. A list of the measures is provided in each discussion of every objective. All of our objectives were supported by the data from CCIT. We had to revisit the list of sub-objectives under each objective. After several iterations, based on our understanding of the objectives and CCIT, the list of sub-objectives was condensed. The following subsection discusses about the refining process of the objectives in details. Further exploration for new underlying constructs from the data was done but no new objectives emerged.

A careful evaluation of each objective was performed based on the evidence from the data to corroborate the claim of CCIT actually meeting that objective. A subjective understanding of various measures employed by CCIT to actually realize each and every objective was also developed. Combining both the evidence as well as the measures suggests an understanding of the objectives in the organization and the management's desire to actually meet the objectives. There were some apparent contradictions noticed in what the management claimed versus what it actually did. These are discussed below.

5.5.1 Refining ISG objectives: Lessons from CCIT

We initially developed 23 objectives and 245 sub objectives in our fist phase of the study. We conducted several interviews and shared our objectives with the managers and the operational level employees at CCIT. We shared and discussed our objectives and sub objectives with two goals. First, we needed to understand if the objectives make sense to CCIT. To achieve the first goal, we generated discussions to understand "how do the proposed objectives influence its security governance practices". Second, we wanted to develop a parsimonious set of sub objectives that could more effectively be communicated for security control design purposes. To achieve this goal, we showed our sub objectives to the respondents and got their opinion on how well the sub objectives, without redundancy, conveyed the essence of the objective. The first goal was achieved by triangulating various sources of data (interviews, manuals, memos, policies and audit directives) at CCIT and critically interpreting it in light of the developed objectives. The analysis was presented in the previous section. All our respondents at CCIT unanimously felt that there was no

redundancy in our objectives. Each and every objective presented a unique and important dimension of information security governance.

Table 5.24 Condensing sub objectives at CCIT

Objective	Initial sub objectives	Final sub objectives
Ensure Regulatory Compliance	Define controls for compliance with regulations Encourage regulatory compliance to internal controls Encourage respect for laws of the society Ensure regulations are followed	Encourage development of controls for regulatory compliance
	Ensure that compliance is a substantive and sustained improvement in business processes Ensure that the regulations are followed Avoid turning compliance into "check the box exercise"	Ensure that compliance is a substantive and sustained improvement in business processes
	Explain the importance and need for compliance to technical people Understand the impact of regulations on controls Formalize process of compliance in the organization	Encourage diverse groups about importance and need for compliance
	Use regulations as a catalyst for better practices Follow regulations in entirety Establish a compliance culture	Ensure compliance is used as a 'catalyst' for security governance

For our second goal, we found that there was a lot of redundancy in the sub objectives. The respondents believed that many of our sub objectives were suggesting the same idea and could be actually condensed into one category that conveys the main theme. For example, table 5.24 shows the case of the objective "ensure regulatory compliance". We started with 14 sub objective in this case. Our respondents suggested that the first 4 sub objectives suggested the same concept, that of encouraging controls development for compliance. So having 4 sub objectives signifying the same thing added redundancy to the objective. In essence all the 4 sub objectives were clubbed or merged to develop one single sub objective "Encourage development of controls for regulatory compliance".

Similarly the last four sub objectives in the middle column pointed towards the same theme of using compliance as means to make security governance better. Hence all the four sub objectives were condensed to form a single sub objective "Ensure compliance is used as a 'catalyst' for security governance". In the same way, we discussed each of the objectives and sub objectives with members at CCIT and condensed the sub objectives for a more parsimonious set of sub objectives. We condensed the initial 245 sub objectives to 88 sub objectives. In one case, we had to change the label of our objective. We initial had an objective labeled "Encourage proactive controls initiatives" (see table 5. 25)

Table 5.25 Changing label of objectives and condensing the sub objectives

Objective Name	Sub objectives	Condensed sub objectives
Encourage proactive controls initiatives	Establish suitable environmental and physical controls	Ensure enough resources for controls
Renamed as:	Ensure adequate resources allocation for maintenance of controls	Enable appropriate environmental and physical controls
Maximize resource allocation for controls	Discourage individuals from feeling restrained due to resources	
	Provide resources for compliance	
	Encourage co-ordination between MIS and accounting for controls	Ensure cross functional group agreement on controls
	Establish controls proactively	

After analyzing the sub objectives, our respondents felt that the label did not necessarily convey the underlying theme of the objective. So the objective was renamed as "Maximize resource allocation for controls" as suggested by the respondents. Again in this case, 6 sub objectives were condensed into three. We believe that our data at CCIT helped us better articulate our objectives and develop a parsimonious and coherent set of sub objectives.

5.5.2 Emergent Issues

Regulatory compliance issues

First issue that emerged is about the organization's stand on regulatory compliance issue. We talked to several people in the management and the signals were contradictory. Explaining the benefits of regulatory compliance, the manager of internal audit division said,

> Regulations are very helpful. It gives you guidelines like there is a blueprint that you are comparing with a real operation to see whether there is a match. If the operation matches the blueprint, that is great. If not, where are the differences? Why are those differences here to begin with? It is very important to have such guidance

Some of the managers agreed that regulations are a big driver for the organization to revisit its internal controls objectives. The regulations helped the organization to reorganize things for the compliance purposes which was helpful as it is something to it should have done anyways. Regulatory compliance efforts helped the organization to achieve the resources that it should have gotten to make the controls better. Compliance helped the organization in providing the much needed boost to improve its control efficiency. With the top management supportive of the compliance efforts, the organization would be able to utilize the opportunity to make lot of changes it wished for. On the other hand, the manager, infrastructure services, when enquired about the regulations as drivers for changes commented:

> No it [regulations] does not drive anything, should it? Probably, I don't think it does because there is no mechanism or there are no means to enforce them. I mean when is the last time you heard that anybody got in trouble for violating HIPAA? Never! Who is enforcing it?

This statement depicts the perception of some of the senior mangers in the organization and also the overall informal attitude of the organization about compliance. Some of the

members of the management felt that compliance is only reactive and take things backwards. Any organization that takes its internal controls program backwards or starts its controls development process looking at the regulations would never succeed in having good security governance. People felt that compliance is the job best left to the auditors. The employees have to participate at the minimum only providing what the auditors need to let them off the hook. The prevalent sentiment in the organization about regulatory compliance is what was shared with us by manger end user services, "They [regulations] are of no help to me but to them [government] it is the right thing to do". Most of the organization did not see any value for the organization in the compliance efforts. But what is the actual state of affairs in this regard for the organization; compliant it is and lots of resources are devoted by the organization in being so.

Internal auditing issues

The second issue that emerged is about the state of internal auditing in the organization. Almost all of the respondents felt that auditing is something very crucial to establish the importance of security governance objectives. The CIO believes that auditing adds to the deterrence efforts and creates a consciousness about the controls. The senior manager added that:

> Auditing is no different to that [as a mechanism to inventory in the military]. They [auditors] come in and they check and look at best practices. We add time to this so that we can follow up on it, so that we are compliant to the direction that we agreed to move on it. They [auditors] need to follow up again based on dates that we customers told them to check if we would meet their recommendations.

The management feels that there are several benefits of performing regular audits within the organization. The auditors, who have industry experience, are in a good position to

assess the performance of the management on security governance issues and provide an independent their party perspective about the state of affairs. The independent assessment assures other stakeholders such as regulators and investors and helps in building the organization's goodwill. Also, the auditors provide a benchmark assessment about the controls and provide a direction for the future governance initiatives. The manager, security, seemed really optimistic about the auditing of the organization and commented:

> I think that if I took over, if I became the CIO, I would be looking at every one of my teams and I would tell them to "prepare yourself" for an audit. I would bring an auditor here and each one of my teams will get audited. That would give me a base line, for me as a new boss to work on. I can only improve, if it got any worse, my job should be gone that's what I would do. Economy improves if the government works well.

Considering the fervor and the emotion attached to auditing by the management, it appeared that the organization was frequently audited and took the feedback from the auditors to improve the security governance process. On the contrary, there are very few audits in the organization and the perception about auditing is not very favorable in the employees. Commenting about the frequency of the internal auditing, manager () shared;

> We have had so far 3 audits. One desktop support, one licensing and helpdesk and I think one was administration. I believe that is all it is. I have been here 9 years. It's [auditing] not frequent. We are pretty much organized and we are not too bad to get it.

Through our observations and informal conversations to the employees and managers, the reason for this apparent contradiction was, to some degrees, clear. It seems that at a typical state agency, auditing, over the years, has been used as a tool to punish agencies that create trouble for the top management. Thus, if a particular department is not following the orders

or doing things in a manner which is not appreciated by the bosses higher up, that department or agency is subjected to an immediate audit. This way the trouble making department is answerable to the bosses 'higher up' for the findings by the audit team. Now, this might not be the case at CCIT. It is possible though that the bosses higher up are happy with CCIT and hence a lack of audit. Whatever the reason might be, it is apparent that perception about auditing in the organization is not a constructive one.

Segregation of duties issues

The third issue that emerged from our data alludes to the organization's position on segregation of duties. The interview data suggests that, for the most part, management feels that segregation of duties as a control is very important for the organization. As shared by the manager, infrastructure services:

> How do you deal with this [internal fraud or security breaches]? Design proper controls. Ensure responsibility and accountability, have multiple layers of controls, segregate duties, have auditing. Segregation of work is important, make sure people in a group just keep doing what they are doing and never cross the line. They should not know about how others do their work.

The security team felt that segregation of roles is a very important control for security governance. It is as important as designing correct access controls and authorization mechanism for the systems because an inadequate segregation of role would provide unauthorized access to people who have no reason to get access to certain things. For example, the developer who writes the code for the application that is used for the meter reading purposes in the City, should not have administrative access to the system. There are chances that if he can misuse the administrative access and get into the production environment and make changes which no one can notice or know. An inappropriate

segregation can be devastating to the integrity of the business processes. The management at CCIT understands this and claims to follow this practice of segregating the roles to the core. As shared by manager administration;

> You have to have internal controls to have separate roles for people so that you know employees are never put in a position that looks like compromising. If you are writing the checks, you are never going to be the one balancing the budget and showing in the checks or something like that. If you are writing the checks, there is someone else to find what you are doing, who tells u how to write the checks, so that if you are absent my business continues to move. In my administration staff, I have done all of it.

But we did get evidence to believe that segregation of the roles are not done all the times. There have been instances where people have had inadequate accesses in the name of cross training in the organization. The manager of administration seemed to understand and know this but was unapologetic nonetheless. Sometimes, in name of cross training, the staff at helpdesk performs the job of assessing the adequacy of their own work. There is a helpdesk team (say primary) that takes request from the city users and there is a team (say secondary) that supports their functions as back up. There is another team (say surveillance) that performs frequent and random checks on the work requests to ensure that all work orders are being addressed adequately. There have been times when the person doing the primary work of support checks his own work the next day in the surveillance team. The manger justifies this in name of cross training. She shares;

> Cross training is your safest bet. You can't have one person with all the institutional knowledge, you will die. You have the take the risk, it's worth it.

This situation can create a major vulnerability for the organization where the primary team members do a fraud and approve the fraud next day from the surveillance team. Many of such issues are overlooked by the management in name of resource crunch and understaffing. It appears that there could be a potential fraud lying somewhere in this organization which in matter of time would be detected. Since nothing has gone wrong so far and all the employees are old and trusted by the manager does not guarantee that things would remain as they are in the future.

In summary, the contradictions proposed in this section remain unresolved. We have suggested, based on our understanding of the organization and its culture, some line of reasoning to make some sense of the anomalies. Currently, a theoretical analysis to explain the anomalies observed at CCIT is beyond this scope of this research. However resolving these anomalies call for a fresh investigation into the matter with new set of research objectives and scope. We intend to work along those lines in the future.

To summarize, the case study at CCIT allows us to empirically reexamine the objectives proposed in phase one of the study. This research, for the first time in information security governance research, proposed theoretically and empirically developed security governance objectives and then validated the objectives through case study data. Some issues emerged from the data which have been documented. The issues explained in this section remain unresolved. We have suggested, based on our understanding of the organization and its culture, some line of reasoning to make some sense of the problems. Currently, a theoretical analysis to explain the reasons for the issues observed at CCIT is beyond this scope of this research.

5.6 Conclusion

In conclusion, the case study at CCIT provided interesting insights into security governance objectives and practices in a real organization. The management in the organization is dedicated to the cause of developing robust security governance practices and thinks proactively about all the aspects of a good controls program. All the objectives developed in the phase one of this study are reexamined in this case study. Most of the objectives are being used in this organization and the remaining the objectives are appreciated by the management and are being considered for their security governance program. We have presented a list of measures that CCIT takes to achieve the proposed objectives and the evidences from the case study in support of the objectives. This chapter presents a list of 6 fundamental and 17 means objectives for maximizing information systems security governance in organizations. These proposed objectives are based on theory, grounded in the values of organizational stakeholders and empirically examined through a case study. The next chapter presents a synthesis of the entire research and answers the "so what" question about this research, both phase one and two.

CHAPTER 6 Interpreting ISG Objectives: A synthesis

6.1 Introduction

This chapter presents the all-important learning for successful development of ISG objectives in an organization, which has emerged from both the phases of our study, Interpreting the meanings and implications of the developed objectives, the principles for good ISG are proposed. The emergent principles are the basic propositions for achieving adequate ISG in organizations. The goal of the chapter is to synthesize our findings and establish its significance by articulating the new insights from the study. In order to articulate the findings, two questions would be answered. First, how can organizations achieve adequate ISG? Second, what are the contributions of this research which go beyond current thinking? The entire chapter aims at answering these questions.

The rest of the chapter is organized as follows. Following the introduction, the second section presents the principles of ISG which are proposed and establishes their significance. A means-end framework for maximizing ISG is presented. In section three, the developed objectives are positioned in context with other leading governance objectives in literature. A discussion is then generated about the relevance of the objectives in the light of other established ISG objectives. Finally, a concluding section is presented with implications of the research.

6.2 ISG principles for organizations

The objectives developed in this research help in increasing the importance of information security governance in organizations. A critical analysis of the data from the study

suggests interrelationships between the objectives and emergent ISG principles. By definition, fundamental objectives help directly in achieving the strategic objectives of the decision context and means objectives lead to the fundamental objectives. Organizations can maximize ISG by achieving the six fundamental objectives. In this section, we present a discussion about how organizations can achieve the fundamental objectives and the principles of ISG. Based on the relationships, a means-end framework is presented.

6.2.1 Defining a Corporate Controls Strategy

Security presents several governance challenges, which require new policies, technologies and organizational capabilities (Gordon and Loeb, 2002; Karyda et al., 2005). These challenges could be in the form of: new unwanted costs for protection of assets, the diversion of resources for controls purposes creating new vulnerabilities; temporary nature of solutions. A controls strategy helps in planning and coordinating in advance to meet these challenges. The strategy for security governance defines the business context in which information security will be managed and prioritizes the resources allocation for the objectives. The real benefits from the information would not be achieved if the information systems and technologies are applied in an unfocussed and piecemeal way (Doherty and Fulford, 2006). The process of formulating an information systems plan helps to explicitly focus the planners' attention on available opportunities for exploiting information (Ward and Peppard, 2002).

There is evidence in research literature pertaining to information security governance which corroborates the relationship between strategy, leadership and management commitment. For instance, Lane (1985) suggests the integration of security into overall

enterprise strategy. Security governance would get its due in an organization only as an enterprise strategy issue. Shupe and Bheling (2006) argue that successful deployment of any IT plan requires management commitment, a structured decision making process and a strategy based on an understanding of the vision and architecture of the organization. The awareness for the need for control strategy is increasing (Shedden et al, 2006). Effective control strategies require efficient risks management processes. Management needs to be committed to implementing an effective risk assessment procedure where vulnerabilities and threats are identified. These can then guide the implementation and monitoring of control strategies and measures (Whitman and Mattord, 2005). Therefore, a structured methodology for developing a strategy will increase the likelihood of success of the corporate initiatives (Shupe and Behling, 2006). Any strategy would fail without consistent support of the management (Wright, 2007). Regular meetings and briefings with the top management keeps the focus on the ongoing nature of security governance for the management and establishes the importance of the controls. This leads to our first principle of information security governance:

P1: Security governance activities shall be planned, coordinated and executed by developing a strategy for controls by the leadership to encourage management commitment for allocating resources.

Security controls planning and resource allocation needs strategic attention. The problem with the existing security guidelines, prescriptions and best practices is that all of these take an operational view of risks. Research literature suggests forward planning for likelihood of attacks and argues that plans, programs and actions that reduce the frequency and seriousness of incidents, reduce risks. More often, organizations take a standard

approach, based on best practices, to controls formulation and deployment. Standard frameworks assume that controls are applied universally, have no strategic influence and are not context dependent.

The strategic management of security controls focuses on the competing demands for enterprise resources and their opportunity costs, and seeks to identify security benefits that justify related costs (Anderson and Choobineh, 2008). At the strategic level of an organization, the benefits of information security (considerable reduction in damages and losses), must be balanced against security costs (Sklovos and Souros, 2006). Expenditures for security that exceed this balance may further reduce expected losses, but may be excessive given their opportunity costs (Gordon and Loeb, 2006). The role of leadership and management commitment is crucial in achieving the controls strategy. Also, resource allocation for security governance is a part of the strategy and can not be optimized without the management's total commitment to the governance program.

Our data suggests that visible executive leadership influences the management to become more committed towards the security governance initiatives. If the leader is committed to governance program, he "draws in" the management and ensures that management provides all the right inputs for controls. For instance, the CIO at CCIT is really committed to the security controls initiatives and it is due to his dedication that the security governance program is effective. As shared by the security manager:

> He [CIO] is supportive of our actions. The hard part is getting to his colleagues, the other directors, who need to approve it but have no clue about it. But we depend on the CIO to get the things done. He helps in getting them [other directors in the city council] on board.

Management commitment is also required for maximizing resources for allocation of controls. The management has to be committed to security governance initiatives for the controls to work as intended. Controls require resources in the form of finance, people and technology. Resources are imperative to be able to develop a dynamic control structure. As we found at CCIT, managers at CCIT rely on their bosses to provide such resources. As explained by the security manager;

> I would recommend going to the top and finding out what the management really wants and then working with those supervisors to find out what it takes to serve that operation everyday. Make things available. You have to have the top on board with the work. Find out what you can do with these resources.

Involving the management in day-to-day activities is the first step in getting their attention and eventually the resources. At CCIT, employees keep the management in the loop about all initiatives and discussions about controls. For example, when the organization needed new resources in reference to the security policies development, the security manager presented all the available resources to his boss. This way the money was made available for the subscription to some firm's website. Research literature also suggests a relationship between management commitment and resources allocated for any initiative. It is managements' responsibility to articulate security risks in a way that resources are not compromised (Wright, 2007). Managers influence the top management about priorities for security governance that includes the induction of adequate skilled and knowledgeable personnel or security specialists. Shupe and Behling (2006) suggest appointing a team to conduct strategic planning for resources to carry forward the control program. Leadership should understand the tradeoffs between high security, usability and cost (Savola, 2007).

These tradeoffs are strategic decisions and should be taken in the planning stage of the security governance program. It is important to involve the managers as well the users in strategic planning about resources. The success of the decisions depend on the operational level management (Savola, 2007).

6.2.2 Developing regulatory compliance within organizations

Regulatory compliance is a crucial aspect of an enterprise security governance program. Emergent from our study, and supported by the research literature, there is a tangible relationship between audit efficacy, business process clarity, deterrence practices and regulatory compliance preparedness. Measuring the compliance preparedness and enforcement has become pivotal to good Information Security Governance in general (von Solms, 2005). In preparing for regulatory compliance, an in depth knowledge of business processes is required. Leading regulations describe specific requirements for various IT related business processes which require comprehensive documentation to demonstrate how personnel decisions implement standards and regulations. Clear business processes help the auditing function fish for anomalies in the systems. Frequent audits can help organization maintain the clarity in processes and also the fear of non compliance. This helps in increasing the probability of being caught in case of deviant behavior. Management needs to evaluate compliance with the regulations to estimate effectiveness and possible shortcomings (Myler and Broadbent, 2006). Auditing can help to determine areas for improvement (Myler and Broadbent, 2006). Given the regulatory environment in IS domain, the importance of security audit functionality is exponentially increasing. An audit process is a strong tool to contrast the policies versus practices of an organization.

Based on the discourse above, our second principle of information security governance is proposed:

P2: Business process clarity should be encouraged through efficient audit processes and punitive structures to achieve compliance.

Auditing deters the creation of anomalies in organizations. By virtue of the fact that they are watched, employees tend to behave in accordance with rules. As suggested by the CIO at CCIT:

> They [auditors] make people honest. If you know someone is watching and will look at what you are doing, you know it makes a difference. Even if you don't look, 90% of the time just the threat that you are going to be looked at, and you don't know when, makes a big difference on compliance. I would like to put this down to human nature.

The clarity of business processes improves efficacy of audit practices in the organization. It is crucial to understand the work flow in an organization such that the controls can be integrated into the business processes in a manner integral to the functionality of the system. Auditors require well understood and established business processes to examine the flow and suggest ways to enhance the integrity of the process. Management should ensure that there are established acceptance criteria for the performance of systems which helps the auditors to check the actual performance of the systems versus the expectations from the system. An assessment of actual versus expected performance of the system helps in testing the accuracy of the data that is provided to the customers in the organization. The verification of the anomalies in the business process requires external intervention in the form of auditing. Auditors can be efficient only if they are able to understand the intricacies of the process and can then suggest how integrity can be restored in the system.

Security governance requires an end to end view of the operations in an organization which can be achieve through clarity in business process. Savola et al. (2007) argue that understanding the dynamics of business processes is crucial for governance purposes. The linkages of security with business process helps in creating knowledge horizontally and vertically in organizations. The vulnerabilities in business processes can lead to breakdown of compromise of the systems, intentionally or otherwise. In such cases, preventive security mechanisms and active deterrence measures protects the organization. Darcy and Hovav (2007) argue that combined proactive and preventive approach to security deters users from IS misuse. Frequent audits are one of these preventive tools. Auditing helps in achieving good security governance providing traceability of user action and a chain of evidence that can be reconstructed to actually understand when and how the system broke down (Swanson, 1996). Audit controls track the operations on file and in-built audit trail capabilities in the software. This helps in accessing logs for pattern of usage. One of the most important usage of audits is to help the organization in meeting regulatory compliance (Goel et al, 2006). Security countermeasures include deterrent administrative procedures (such as frequent audit) and preventive security software, lead to lower computer abuse (Straub, 1990).

This study also shows that regulatory compliance requires standardization of the controls such that the stakeholders of the organization are able to trust the management with critical information. Clarity of controls development is a must for actually standardizing controls and establishing trust within and outside the organization. Regulations are basically intended to protect the interest of external stakeholders, such as the investors and the

business partners. Standardization of the controls is one of the best strategies to proactively establish respect for the organizations security program (May 2005). Loss of trust and confidence which results from an organization's inability to meet the expectations of users and to protect their identity and privacy would compromise business objectives. This leads to our third principle of ISG:

P3: Standardization and clarity in controls should be developed to enhance trust within and outside the organizations and to achieve regulatory compliance.

Regulatory compliance helps organizations do things in a manner that is consistent, transparent and open for review. Clarity in controls development process assures an expected pattern of behavior which leads to enhancing intra-organizational trust for security measures (Dhillon and Backhouse, 2001). Trust is an indicator of a series of direct relationship with people and not with a series of organizational entities or polices (Fleming, 2007). If there is lack of trust in the organization, regulatory compliance would be compromised and would be not entirely in the spirit of the legislation. Standardization of controls helps in trust building both within and outside the organization. The standardized control and established procedure for security governance facilitates the communication process within the organization and outside it, with other agencies. The management should encourage standard protocols for controls development as it makes it easier to find the deviations in the systems and help in covering any vulnerabilities. As shared by an internal auditor from energy industry:

> An organization should regularly compare and analyse its security state, investments, and actions in relation to others in its market sector and community of practice.

Standardized controls help in ensuring that expectations on the stakeholders' part are being met. In case of non compliance with agreed procedures, the standardized controls structure also communicates the need to be compliant and consequences of non compliance. Research literature suggests that one of the main purposes of having standards is to ensure effective trust with stakeholders.

Clarity in control development process leads to trust building mechanisms as well. Clarity and transparency in control development process helps end users in understanding the need for the controls for security governance and their individual roles in fulfilling the need. At CCIT, through clear controls development, the management conveys that it wants to protect the employees from committing avoidable errors through sheer ignorance. The management also provides support in clarifying the doubts of the end users about the controls. As shared by the security manager,

> If you don't understand anything, then HR may be the one place you go. I [an employee] don't understand what it means, I ask this upfront. Having to own the policies, it [the management] should be responsible for the procedure, be responsible for answering those questions. Clarifying the concepts helps people to believe in the governance program in the management.

The practice of supporting employees' efforts to understand controls establishes an environment of trust in the organization. Top management should ensure that there is a formalized route available when employees have doubts about controls and they should be able to get the confusion cleared. This also assures the employees that the management wants to protect them from causing unintentional harm and getting into trouble, and that it is actually protecting the employees. Also clarity in controls helps other business partners to identify with the controls and trust the management to take due care of the critical data.

6.2.3 Defining continuous improvements for controls

In this research, continuous improvement of controls has emerged as a key requirement for adequate ISG efforts. One of the important aspects of information security governance is testing and validating controls against business requirements. Business needs are dynamic and change with time and so should the controls which are designed to protect this information and processes. A change in the business needs should be reflected in the corresponding controls. This can be achieved by regular monitoring and feedback on the controls, by providing adequate training and education to the users and by communicating the changes clearly inside the organization. The monitoring and review of controls post implementation is a critical phase for success of the overall controls program (Shedden et al, 2006). End users should be able to understand the changes in controls so as to be able to use the systems properly. This can be achieved through developing open communication policies where discourse about controls is encouraged. The employees should be willing to comply with the use of the controls. A monitoring technique can be effective only if the employees understand and are willing to use the controls and provide feedback (Booker and Kitchesn, 2006). This willingness can be increased through training about controls and communicating the uses and needs for the controls. Straub and Welke (1998) suggest feedback leads to develop better communication channels through departmental meetings and informal chatting. The results in this study suggest a healthy relationship between frequent communications, regular monitoring and feedback and training and education with continuous improvement in controls. This leads to our fourth principle of ISG:

P4: Frequent communication should be encouraged through regular monitoring and extensive training for iterative development of controls

Monitoring and feedback channels in the organization add to the effectiveness of communications about controls. Management needs to constantly revisit the controls based on the feedback from the employees. The feedback needs to be communicated in a way that it is actually incorporated in the next iteration. The security officer at CCIT articulated this best when he said:

> We need to constantly monitor and develop an evolving environment which is changing continuously. I mean this can be done through talking to people, by communicating properly and then actually going and constantly modifying it based on what they say.

Training and education improves communications about controls. Training, specifically about controls, emphasizes using knowledge about the relevance of controls in daily practice. The end users should be adequately trained and educated about usage of controls. The knowledge thus imparted leads to more enquires and frequent communications about the controls. As the security director said:

> Make things very clear to the employees, these are our policies, these are our procedures and controls and these are our expectations. It is essential to communicate this. Education and communication are absolutely vital.

Training in security controls create effective communication channels and facilitate open discussions and debates of important issues about controls. Regular training helps in surfacing the lack of knowledge about the security and control issues and effective communications help in resolving those issues.

This study also suggests a relationship with resource allocation, clarity in control development and formal controls assessment functionality in achieving continuous

improvements in controls. Resources are required to institute changes in the governance structure. The acceptance of the changed and improved controls would be enhanced when the process of control development is open and transparent. This clarity in controls development process facilitates quicker adoption of the changes being introduced in the governance program. Instituting controls assessment functionality ensures that all the control initiatives are centralized and adequate budgetary allocations are appropriated for security governance purposes. One of the major drawbacks for controls program has been the lack of resources. The centralized functionality ensures a cost benefit estimate of the controls for long term benefits. This leads to our fifth principle of ISG:

P5: Controls development shall be clear, transparent and easily understandable to the organizational members' and adequate resources need to be allocated to institute formal controls assessment functionality.

At the strategic level of an organization- the benefits of information security (reduced damages and losses) must be balanced against security costs. The strategic management of security focuses on the competing demands for enterprise resources and their opportunity costs, and seeks to identify security benefits that justify related costs (Anderson and Choobineh, 2008).

Resource allocation for controls is required for developing formal controls assessment functionality in an organization. Resources for controls are always an issue as controls assessment is not a separate functionality and no department owns up this cost. As explained by the security manager CCIT:

> The biggest problem is that controls have limited resources. We want to do so many things but can't do it. Like it [controls] needs to be constantly modified and

> monitored but that [modification and monitoring] needs investment. Do we have separate money for this as a department? No-we are always facing a cash crunch.

Adequate controls always require good resources to protect business integrity. However good the security governance plan is, if there are no resources to support that plan, not much can be done. As explained by the security manager in a healthcare industry:

> Everything comes down to the cost of the risk. How do you balance cost of the control versus the risk? Risk is great; and cost of control may be worth it. How do you balance cost of the risk to the control?

Resources would be available if there is separate controls assessment functionality with individual controls budgets. Developing control assessment functionality is a new concept introduced by this research and currently does not have any support from research literature.

Clarity in controls development also helps the cause of creating formal control assessment functionality. Our data suggests that if there is clarity in how controls are being defined, it would be easier to have a formal controls assessment entity that could validate the requirement of the controls and provide adequate support for it. As explained by a senior manager, software development, in financial services industry:

> Clearly define the requirements and then you get everybody who is involved to agree on those [requirements] and then from there, you build out your processes. You need to formally integrate the requirements into the controls and do periodic assessment of these [controls].

Lack of clarity in controls can lead to vulnerabilities endangering systems. Formal controls assessment functionality looks into the possible vulnerabilities and seeks solutions to deal with the threats. As explained by a manager, purchase department, electronics industry:

> If you suspect what is generated is not right, then you should investigate instead of giving a blanket approval to all transactions. This is where assessment of controls is required, does it work?

There exists a pressing need for developing a formal control assessment functionality which can centrally manage the information security governance activities.

6.2.4 Establishing a controls conscious culture in organizations

Control conscious culture is achieved when the implicit knowledge about the security controls starts guiding the day-to-day activities of the employees in the organization. This entails that controls have to become the part of the corporate culture (Thomson and von Solms, 2008). Controls have been internalized by the employees and have been accepted at an informal level of management as well. This state of security governance can be achieved if the individuals are able to align their values about controls with those of the organization. The controls culture is crucial for security governance as it can act as a powerful, underlying set of forces which establishes individual and group behavior within an organization (Schein, 1999). Encouraging group cohesiveness helps in propagating the right values for security controls. Our study suggests that controls conscious culture is facilitated by strong communications, cohesive groups and alignment of individual and organizational values about controls. This leads to our sixth principle of ISG.

P6: Controls consciousness shall be developed through regular communications and forming cohesive groups which leads to alignment of individual and organizational values.

Management should espouse similar values to those it practices in order to help employees identify with the organizational values about controls. If the beliefs and attitudes of the employees are addressed by the management, it leads to changed actions and behaviors of

the employees and synchronizes with the overall corporate security culture in the organization (Thomson and von Solms, 2008). If there is alack of alignment several problems occur such as miscommunications and lack of cooperation from employees (Sathe, 1993). Hence communication channels should be established and debating the controls in the open should be encouraged. Normative controls would always be required to hold together the security governance initiatives and these controls comprise values, belief systems and culture for the individuals (Dhillon, 2001). Communication activities with the stakeholders are critical for controls (AS/NZS 4360, 1999; Bandyopadhyay et al, 1999). Fuller et al (2007) suggest that there exists a positive relationship between interactivity and knowledge retention about information assurance in an organization. The interactivity is best facilitated by open communication. Establishing controls culture requires enhancing group cohesiveness in the security teams. This allows a coherent interaction channel with the management. A team approach to information security is absolutely necessary if an adequate level of information security is going to be achieved (Wood, 2006).

Establishing open communication polices about controls helps in individual and organizational alignment of values and maximizes group cohesiveness. Effective communication practices help in explaining management values and ideology in a way such that users can identify with the organizational values for controls. To ensure an alignment of end user values and organizational values, it is critical to communicate about the policies, procedures, controls, strategies and controls. As explained by a security manager at CCIT:

> Communication is important but the hard part is to ensure that users continue to listen to you. Something that is going to bring the users on board ought to be helpful so that the users can find it appealing. Something they can identify with, so yet again their values come in play.

Communicating about controls develops clarity about their intent and scope. This clarity is required for individuals to understand what is expected from them and whether it is something that they can or want to do. At CCIT, the controls were made appealing to the end users by communicating something which makes their work and life easier; it's about them and not the bosses. Communication plays can important role in bridging the gap between individual and organizational values about controls.

Communications also influences the group cohesiveness in the functional groups. Managers should encourage frequent communications with their groups as it makes the group 'tight'. At CCIT, inter group communications about controls and security related responsibilities make the groups more cohesive and the managers strive to protect their group members against all odds. Cohesive groups influence the behavior of the individuals in the group and there are chances that individuals will better align their values with those of the organization in the realm of security governance if the groups' values are aligned. It is evident at CCIT that the individual adopts the groups' values about security governance as their own. Their perception about security controls is almost the same as their groups' perception about security governance. The management should understand these needs of the individuals and always "sell controls" to the end users as something to protect the users from harm due to ignorance.

6.2.5 Establishing clarity in policies and procedures in organizations

Higgins (1999) argues that the information security 'policy is the start of security management'. The strategic information systems plan is a critical prerequisite for policy formulation (Doherty and Fulford, 2006). Information security policy is the basis for the dissemination and enforcement of sound security practices, within the organizational context (Baskerville and Siponen, 2002; Doherty and Fulford, 2005). David (2002) argues that formal policy is a prerequisite of security. Similarly, Lindup (1995) asserts that security policies are the foundations of information security management. Establishing data criticality requires clarity in policies and procedures. Efficient audit process and clarity in controls development help in achieving data criticality. An audit process is a strong tool to contrast the policies versus practices of an organization. Our results suggest that clarity in policies and procedures can be achieved through data criticality, frequent audits and clear controls development process. This leads to our seventh principle of ISG:

P7: Data criticality shall be established by ensuring frequent audits and a transparent controls development process to enhance clarity in polices and procedures.

Audit provides traceability of user action and chain of evidence that can be reconstructed to actually understand when and how the system broke down. Real time auditing can also help in detecting other problems in the system other than break downs, thus ensuring the data integrity, confidentiality and availability. Controls, where possible, should be transparent or viewed as positive contributions to job performance. Complex controls that increase constraints on people should be minimized (Parker, 1996). Clarity in controls development process and incorporating controls in systems development would lead to better technical controls and thus enhance data criticality (Dhillon, 2001). Separation of

duties between developers, testers and administrators in operational facilities reduce risks of unauthorized actions (Myler and Broadbent, 2006). This separation is ensured by audit functionality. Thus frequent audit provides users with confidence in the integrity of data. The end result is trust in the IT infrastructure which is really valuable in today's business world (Tickle, 2006).

Audit efficacy leads to ensuring data criticality. It is essential that these controls and access are constantly revalidated and checked from an independent perspective. This is where the important role of auditors comes into play. Segregation of duties, right access and adequate authorization mechanisms are required for data criticality. Auditors ensure that these mechanisms are sound and work for the organization. As the internal auditor at CCIT suggests:

> Is it possible for developer to go into production data base and goes to his or her own household and reduce consumption by 50% every month? If that's possible and then you get audit break down, you have a controls breakdown. So whenever you have people that have unwarranted access such as developer has access to production, we [auditors] need to come in.

The efficacy of audit practices depends on how well the auditors are able to protect the data in the system. Auditing ensures that during changes in roles, access to information is changed as well. Auditors bring in a lot of experience and knowledge about best practices, suggest changes which are important and follow up on the implementation of those changes. Clarity in controls development process also helps in establishing data criticality in an organization. To maintain the confidentiality, integrity and availability of the data, it essential to develop clear controls for access, authorization, classification and segregation of duties in data usage. Also, change management controls are crucial in ensuring

criticality, which can be a potential source of threat to an organization. At CCIT, the management makes sure that people follow the controls or else they would be kicked off from the systems. This requires that everyone be clear about the controls and the business process, which help in establishing data criticality.

6.2.6 Establishing responsibility and accountability structures in organizations

It is important that organizational members own up the responsibility of their actions and are accountable for their decision for the success of any security governance program. Responsibility and accountability in structures requires visible leadership that motivates people to be responsible in their jobs and take the blame for their actions. Leadership can set an exemplary ethical and moral environment which allows the members to trust the management about its intentions. Increased awareness and individual accountability can greatly affect how security practices are implemented in an organization (Mellor and Noyes, 2006). This study suggests that responsibility and accountability structures is established in an organization with the help of leadership guidance, ethical and moral tone, punitive structure and trust building measures. The research literature supports this relationship. This leads to our eighth ISG principle:

P8:Trust building measures shall be appropriated through executive leadership and punitive structures to establish the right ethical tone for the organization for the assigning of responsibility and accountability in its structures.

Corporate boards, that undertake the challenge of IT oversight, show that they understand the scope of their corporate accountability and responsibility, and are proactive in their leadership duties (Myler and Broadbent, 2006). To establish trust and ethical conduct, leadership should be able to “walk the talk” and espouse controls that are important and

then follow these personally (Drennan, 1992). It is the part of executive duty to set an exemplary ethical and moral conduct for the employees to follow (Thompson and von Solms, 2008). Senior managers can communicate policies and codes of ethics to guide employees (Krull, 1996). It is the responsibility of management to serve as a role model for the behavior it wishes to promote (Krull, 1996).

Information Systems professionals generally demonstrate a solid understanding of information security ethics as they apply to organizational goals (Pearson et al. 1997). Normative controls aimed at guiding the ethics and morality in the organization are important. The security technology design often neglects the moral or ethical element of the governance process which is one of the most important aspects of security management (Gupta and Sharman, 2008). Dhillon and Torkzadeh (2006) suggest that instilling value based work ethics would help in ensuring an ethical environment which will lead to employees abstaining from unacceptable behavior and a secure organization. Mutual trust between employees and management is important to ensure that responsibilities are internalized by the employees. Lack of trust in policies and procedures can make the employees alter systems and simply not comply with controls such as not sharing passwords or taking confidential data out of the office on laptops (Booker and kitchens, 2008). Punitive structure also helps in acceptance of ethical codes in the organization. For maximizing deviant behavior, it is best to reinforce positive beliefs and attitudes. In other words first clarify what behavior is acceptable through clearly establishing the ethics and morality valued in the organization.

Ensuring ethical and moral values helps in establishing the punitive structures in an organization. The ethical environment in the organization creates normative pressure on the people to do the right thing and not break the law. Personal values and morality shapes an individual's tendency to conform to the laws and rules. As explained by the manager infrastructure manger at CCIT:

> So we can make a rule, we can make a law that you have to be honest. I mean, in reality, our personal values, our own values should define that we are going to do the best we can, do the right thing at any point of time. If my personal values allow, then only will I follow the rules. My personal belief is that you can't legislate that, you can't provide enough legislation to do that.

Visible executive leadership helps in propagating ethical and moral values in organizations. Executives in visible leadership positions should lead by example. This is exactly what the administration manager at CCIT does. Leadership also leads to trust building mechanisms in an organization. The executive leaders, who build the controls, need to be trusted by the employees who actually use the controls. As security manager CCIT explained:

> It's very complex [developing controls]. Reach out to HR, legal people; get all resources to learn from them. Draft things that can actually work for everyone. You need to take all stakeholders in confidence, win their trust, and ensure that you are working for them [individuals] not against them. It is what they need.

Leaders have to win the confidence and trust of the stakeholders to successfully implement the security program. Thus we postulate that visible leadership leads to trust building in the organization. Research literature in this area supports this claim.

Our study suggests that establishing punitive structures helps in trust building mechanisms in an organization. Clear punitive structures in an organization establish the fear of

consequences of non compliance with the rules. This environment leads to the formation of more trusting relationships between employees and the management. The employees need to clearly know what's acceptable and that it's their personal responsibility to make sure things do not deviate from normal behavior. It provides a fallback plan for the employees where they know they can trust the management to be fair and just, in cases of beaches which are not their fault.

Management should ensure that all the policies and procedures are easily accessible to employees leading to clear deterrence criteria. Having established the boundaries for the employees, management facilitates an environment of trust by relying on the individuals' sense of responsibility to do the right thing every time. It is important to establish the framework within which individuals can be flexible with work responsibilities. There are equipments lying around at CCIT without any extra precaution or surveillance to protect them from theft but nothing has gone missing ever. This is because people trust each other and know what happens if they get caught. Deterrence leads to trust not only within the organization but also for the outside stakeholders such as investors, regulators, partners, possible clients and employees.

In summary, based on data from phase 1 and phase 2 of this study, we developed a means-end framework (Figure 6.1) for maximizing information security governance objectives in organizations. The paths in the diagram show a directional preference. The relationships are postulated based on our understanding of the data, observations at CCIT and the extant research literature in information systems security governance area.

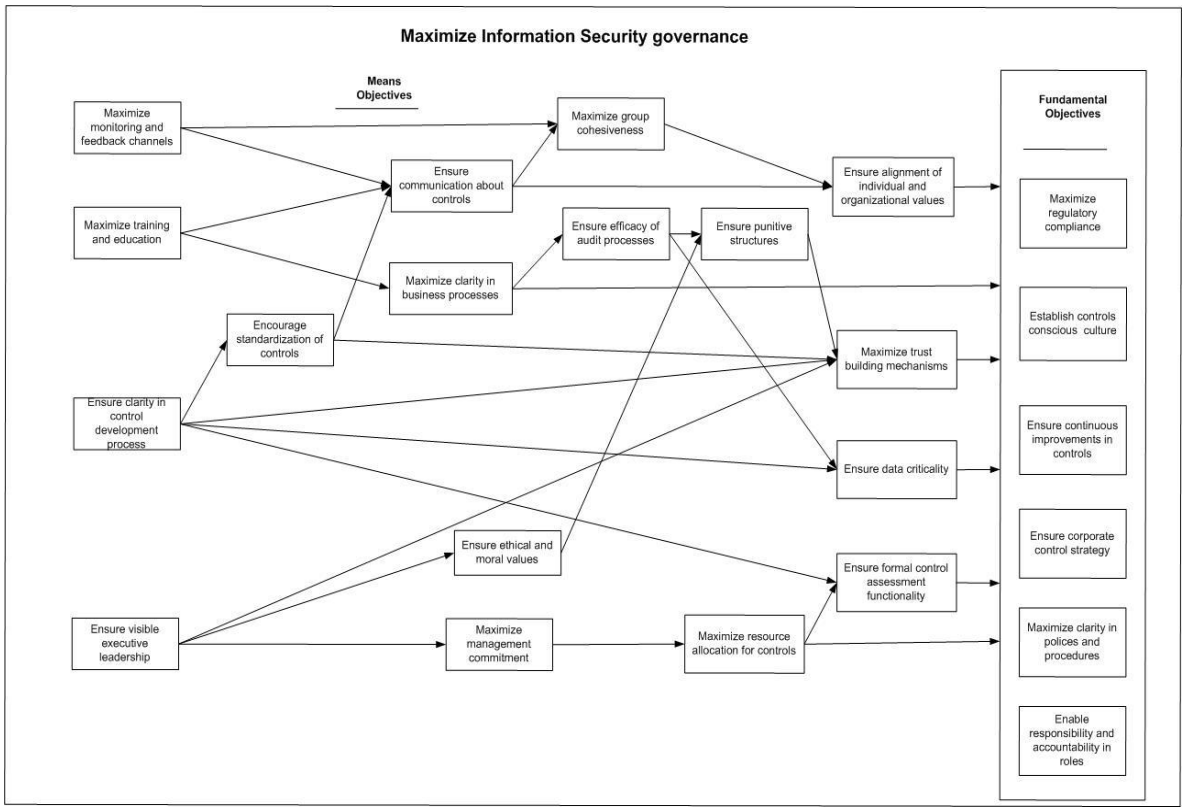

Figure 6.1 Means-end framework for maximizing information security governance

The framework contains six fundamental objectives integral to maximizing information security governance in an organization. There are seventeen means objectives that add to these fundamental objectives and play a subsidiary role in attainment of the final strategic objective of maximizing information security governance. A detailed discussion on the implications of the fundamental objectives and ways to achieve these objectives is presented earlier.

6.3 Discussions

The key to setting the right controls is defining the correct control objectives. In order to know if a control is effective or not, the first questions that the management should pose is, "Do we have the right objectives?" (Galloway, 1994) Considering the importance of

having the right objectives, this research suggests a set of control objectives that have not been articulated, emphasized or used in information security research. All the objectives developed in this research are rooted in the research literature for information systems security, information systems security governance and related disciplines such as strategy, management, psychology and sociology. The cross functional nature of security governance needs to justify the inputs from other disciplines. While most of our objectives have been acknowledged in the extant literature, some of them have not been emphasized enough. Objectives such as "establish control strategy", "establish deterrence criteria", "establish clear control development process", "establish formal control assessment functionality", "ensure efficacy of audit processes" and "enhance group cohesiveness" call for special attention. Our analysis suggests a crucial role of the above objectives in information systems security governance. Neither the commonly used security management standards nor the available security governance models highlight any of these above objectives. These objectives seem like anomalies in the commonly used governance frameworks. A search for the word anomaly in dicitonary.com shows "a deviation from the common rule, type, arrangement, or form". There is little support for the above objectives in security governance area. Hence, we propose these objectives as "theoretical anomalies" since the governance models have not mentioned these objectives. It should be noted though that some of the sub objectives of the above mentioned governance objectives do get mentioned in the research literature (see chapter 4 for discussion of above objectives). But none of the available frameworks argues for the above objectives specifically. We feel

these objectives are important on their own and need to be considered for comprehensive governance programs. Each of these five objectives is briefly discussed below:

Issues and concerns with a corporate control strategy: Control strategy is required to understand the security governance environment and how it fits with the overall organization's business strategy. Organization's security requirements should be driven by enterprise requirements and the solution should fit enterprise processes such that strategic benefits are realized (Anderson, 2001). Control strategy helps in aligning security investment with enterprise strategy and agreed upon risk profile. There should be an alignment between the organization and its control environment. The alignment process involves arranging internal structures and processes in a way that people can come up with creative strategic alternatives and develop new competencies to meet the challenges of the future (Jemison, 1981). We have seen that organizations are increasingly using management control systems to enhance their strategy process (Simons, 1995) as controls may be used as agents to secure strategy implementation (Marginson, 2002). Simons (1994) posits that control systems are used by management to overcome organizational inertia, communicate new strategic directions, establish implementation timetables and ensure continuing attention to new strategic initiatives.

Realizing the importance of controls in the overall strategy of organizations, it seems logical that developing controls strategy goes a long way in establishing effective security governance. At least out data suggests that it will. But there has been no clear call in information security research for establishing a control strategy or in practice.

Issues with creating punitive structures: To enforce the controls effectively, it is indeed important to establish two things upfront; what non conformity with controls could mean and what are the consequences of non conformity? As observed by a respondent:

> None of these control measures will work if key individuals and the organizationlack the fortitude to enforce the rules and the remedial solutions [internal audit director, federal agency].

In situations of strategic change, control systems are used by managers to formalize beliefs, set boundaries on acceptable strategic behavior. Deterrence criteria shape the perception of the workforce about "what is expected" from it. Clearly establishing the expectations of the organizational members reduces the pressure from the management in explaining right from wrong. Establishing deterrence criteria should also include defining and measuring critical performance variables and motivating discussion and debate about strategic uncertainties that help organizations pass through changes (Simons, 1994). Research in security of information systems has acknowledged the importance of establishing deterrence criteria for enhanced enterprise security. Dhillon and Torkzadeh (2006) argue that deterrence is an important objective for maximizing security in organization. Straub and Welke (1996) have used general deterrence theory for establishing the need for deterrence activities in the organization. But there has been a lack of effort in information systems security governance research to establish deterrence as an important objective for governance. This research puts a stake in the ground and argues for the establishment of deterrence criteria for effective security governance. This study suggests that rewarding conformity and punishing non conformity with controls can actually help the organizations in managing security. This is identified as a theoretical

anomaly since most of the information security governance frameworks do not include this objective.

Issues with establishing clarity in control development process:There should be transparency in control development process. Clarity in control development process increases the probability of all stakeholders having a clear understating of the intent and scope of the controls. Simon (1994) argue that clear controls and procedures and designated liaison roles along with a strong, comprehensive code of conduct and more contingent pay for more employees are associated with fewer occurrences of crime. As voiced by one of the respondents:

> First and foremost information systems are, or contain, property that is a group asset. It is important to establish how individuals charged with its security (often everyone in an organization) value and take care of property that is not their own. The designed controls convey the message, "do your job properly and protect your asset". Controls should be clear in this [Chief executive officer, financial services industry]

To our knowledge, there has not been a single information security governance framework that emphasizes clarity of controls development as an objective. Control development process should be integrated with the business processes such that each and every control developed answers a clearly established need in the business process and the cost of not complying is obvious to the users. This is an important finding of this research and calls for acknowledgment from researchers and sincere efforts to establish it in common practice.

*Issues with establishing formal control assessment functionality:*Anthony (1965) defines management controls as the process "by which managers assure that resources are obtained

and used effectively and efficiently in the accomplishment of the organization's objectives (p. 17)". As suggested by our data, in order to realize this role of controls, formal control assessment functionality should be established. As a separate department, controls functionality would be in a better position to attract enterprise resources, develop better oversight capabilities, assess the needs for controls, monitor investments, get the requisite attention of top management and influence the corporate security culture. To our best knowledge, no information security governance framework has suggested a separate controls department. This study found that establishing formal controls functionality would exponentially boost security governance efforts and a step of this proportion is long over due. As one respondent opined by a respondent

> What makes a car run? what makes it fast? Brakes! you are never growing to drive a car fast if you do not have breaks. Lot of people use security controls just like brakes. In fact, the security controls itself means that the business can run faster, you do not have to worry. That's light ball for a lot of people, security controls agency, Virginia].

Controls should be integrated with the business processes. Considering the impact that controls have in managing business, a call for formalizing a separate entity for controls is warranted.

Issues with enhancing group cohesiveness: Cohesive groups implementing and using security controls can be more effective than groups which are dominated by rivalry, politics and favoritism. Security initiatives call for cross functional collaboration and it is important that the members on the group view the group favorably. As Anthony (1988, pp. 10) mentions, management control can be considered as 'the process by which managers influence other members of the organization to implement the organization's strategies'

(Anthony 1988: 10). Such influences are perceived positively in a cohesive group. This aspect of security governance has not been highlighted in research literature and increasing "group cohesiveness" as a governance objective has not been proposed so far. As observed by a respondent:

> Again sharing comes into play. We all must be able and capable of trusting everyone in the organization that comes into contact with our shared assets. The ability to maintain confidence is a good measure [Director of integrated systems security in public safety industry].

Many of the security initiatives fail due to lack of coordination between various functionalities (Wood, 2006; Fleming, 2007). Organizations tend to repeat mistakes and do not learn from their experiences as there is a lack of alignment between various occupational communities within itself (Schein, 1996). The operational and midlevel managers have different shared assumptions and objectives which are not aligned with the objectives preached and practiced by senior managers. Taylor (2006) argues that it is management's misperception of risk causing behavior and its technology based approach that ignores human factors that must be addressed for increasing security. Considering the importance of group behavior in success of security initiatives, it seems fair to raise a voice for group building efforts and incentives.

All the five objectives discussed here are important for security governance. Though some of these objectives have been alluded to by the researchers but there has not been enough emphasis to any of these objectives in information security governance research. These objectives clearly, play crucial roles in holistic information systems security governance.

More research is required to understand the incorporation of these objectives into organizational security governance frameworks.

6.4 Conclusion

This chapter synthesized the results of both the phases in this study and the implications drawn from this research. The emergent principles of information security governance from the proposed objectives were identified and its implications for research and practice were discussed. A means-end framework was constructed based on the data from the study and research literature available in this domain. This study presents some information security governance objectives that have not been identified in the research literature. These "theoretical anomalies" are listed and implications are drawn.

The following chapter will summarize the findings and review the entire thesis. The theoretical contributions, methodological contributions and practical contributions shall be discussed. A discussion on possible criticisms of the research approach and design will be raised and conducted. Potential future research directions stemming from this research would also be discussed.

CHAPTER 7 Conclusion

7.1 Overview of the research

This research argued that information security governance objectives in information systems need to be grounded in the values of the organizational stakeholders. This argument is based on the premise that if the values of the employees in the organization are reflected in the security governance objectives; then there are better chances that the objectives would produce the intended result i.e. better security. The motivation of the research lies in the fact that there is hardly any work in information security governance area that presents security governance objectives which are theoretically grounded and empirically validated. This research is the first serious attempt to develop security governance objectives that are theoretically established and empirically validated in an organizational context.

On the practical side, this research is motivated by the lack of sound ISG objectives in organizations, leading to catastrophic losses due to misuse of information. Security breaches cost billions of dollars in direct losses, downtime, stolen identities and intellectual property thefts. Fiascos such as demise of the Barings Bank, Kidder Peabody's inability to institute adequate internal controls and Enron's failure to ensure integrity of business processes points to the increasing importance of governance structures. At a high level, governance structures created specifically for ensuring information security are called information security governance (ISG) practices.

There are several models such as COBIT, COSO and ISO 2700 available in the industry to guide organizations towards sound internal control structure. These models are popular and

widely used. But the cases of security breaches due to inadequate controls being unable to prevent these breaches are increasing. This situation calls for a serious revisit of these models, with respect to organizational objectives for providing adequate information security governance to protect assets. An assessment of the contemporary frameworks for internal controls suggests two problems with the use of these models. First, all the existing frameworks reviewed are atheoretical, based on experiences of the originators of the models themselves and derived from best practices in the industry. Second, none of the above frameworks provide guidelines specific to the creation of objectives of internal controls for information systems security. Either the focus is too broad covering much more than security or the guidance is not enough about using specific controls. Review of the research literature in internal controls for organizations does not shed much light on the process of creation of internal control objectives for information systems security. Internal controls for information systems security literature lack the rigor of a theory to guide research in this area. Research in information systems security area does not provide an appropriate theoretical basis to design internal controls for security. In conclusion, a review of internal control objectives, both in research and practioner worlds, suggests a need for a theoretical basis for internal controls. This will help to develop sound ISG objectives for dealing with security vulnerabilities. This research fills the gap by developing value based, theoretically grounded and empirically validated ISG objectives.

This research was conducted in two phases. In the first phase, a value focused assessment was performed to develop information security governance objectives. Value Theory was used as theoretical basis and value focused approach was used as the methodology to

develop 23 value based governance objectives. For this phase of the study, 52 semi-structured interviews were conduced across 9 industries to elicit the values of people about security governance. These objectives which were well grounded in theory, were first of their kind to be developed in information systems security governance research. The developed objectives were clustered in two groups as suggested by Keeney (1992), namely fundamental and means. The objectives that directly help in achieving the main objective for the decision context are fundamental whereas the objectives that help in achieving other objectives leading to the fundamental objectives are called means objectives.

In the second phase of the research, an interpretive case study was conducted to validate the proposed objectives in an organizational context. The single case study was conducted at the department of IT for a major city in central east coast of the United States. The study was completed over a six month period time from October 2007 to March 2008. The data collection methods primarily used in this phase were semi structured interviews, forms, reports, manuals in the department and through informal interaction and observations. Each objective proposed in the phase one of the studies was used to describe the case situations. Some apparent contradictions were observed between what the management said should be done versus what was actually going on in the organization. These contradictions are documented.

The findings indicated that all the objectives developed in phase one are important to the organization. All the objectives were supported by the data and the organizational measures to achieve these objectives were noted. Based on the data from the case study and the conceptual understanding of the researchers, a means-end framework was

developed. The data also suggested eight emergent information security governance principles. These principles are more like directives for organizations and can be used to design control related activities and tasks which will result in maximizing ISG.

The remainder of the chapter discuses the contributions of this research, the evaluation criteria to establish the rigor of the study, the research design limitations and finally the future research directions stemming from this work. Each of the above mentioned topics are presented in a separate section.

7.2 Contributions

Any research endeavor should add to the body of knowledge in the subject area, to be deemed as legitimate. This research adds to the research literature in theoretical, methodological and practitioner streams. A discussion on each category of contribution is presented below.

7.2.1 Theoretical

This research makes a unique contribution to the information security governance field. It is a serious attempt aimed at formulating theoretically grounded and empirically developed and tested information security governance objectives. In this research, the objectives developed are grounded in the values of the organizational stakeholder and empirically validated through a case study. Since most of the models used for security governance are atheoretical and lack scientific support, the objectives developed in this research would be a significant addition to the body of knowledge in this domain. Also, there has been almost negligible research in the area of development of security governance objectives. The developed here should fuel further inquiry in this area.

Second, the means-end framework presented in this research postulates relationships between the objectives and is a theory development exercise. The suggested theoretical framework, based on data from the case study, is exploratory in nature and adds to the theoretical knowledge in information security governance area.

Third, this research brings into light some subtle nuances of security governance that have not been emphasized in the research literature currently. For instance objectives such as: ensure clarity in controls development processes, ensure corporate control strategy, ensure punitive structures, ensure formal control assessment functionality, and maximize group cohesiveness. The above listed objectives have not been proposed as important ISG dimensions in most of the ISG frameworks available, both in theory and in practice. There have been passing references in literature about these objectives but most of the research in this area has ignored the importance of these objectives for overall success of the security program. We believe that these objectives are important in their own right and contribute greatly towards maximizing information security governance in the organization. These should be considered with other controls objectives for overall security governance maximization.

Fourth, Value Theory provides an appropriate ontological and epistemological basis to elicit, interpret and structure individual values for better information security governance research. Using a theoretical lens such as Value Theory from the field of sociology to investigate information security governance issues has provided a rigorous platform for further research in this area. Bringing theories from other disciplines and applying them to information systems domain is a theoretical contribution to the field (Weber, 2006).

7.2.2 Practical

This research has contributions to offer organizations working on security governance issues, mainly in four areas. First, it provides a sound list of security governance objectives that are comprehensive and ready to use. Even though, there are other available security governance frameworks such as COBIT that can be used by corporations, this framework is exclusively targeted at security governance purposes.

Second, this approach allows the end users to participate in security governance programs. This allows a better alignment on user and organizational values. For practitioners in the real world, this framework provides guidelines about the importance of incorporating employee's perspective into control design to ensure better results of security governance initiatives.

Third, a security governance assessment tool can be generated using these objectives and values. An artefact or a tool that can check the current level of security governance in organization vis a vis where the level should be is based on the values of the employees in the particular organization.

Fourth, the ISG principles proposed in this research are like directives which can be used to achieve the objectives proposed in this study. Organizations can use the principles as a high level plan for ISG and develop specific activities to meet the objectives.

7.2.3 Methodological

This study also provides methodological contribution. Value focused approach provides an adequate methodology for empirical investigation of values. This approach is suitable for qualitative as well as quantitative techniques of research. Using this methodology in the

context of information security governance is a contribution to the body of knowledge in information systems security research. Using this approach to develop decision objectives allows better communication between stakeholders and facilitates a "bottom-up" approach to management.

7.3 Evaluation of the research

This research was evaluated using Klein and Myers' (1999) principles for evaluating interpretive field studies. Klein and Myers' suggest providing a summary of the research method, site, theory and key findings before actually assessing the work. This research was conducted as an interpretive field study in the IT department of a state agency. The theory behind the work is Value Theory, which is widely used in Sociology. The findings are 23 information security governance objectives and 8 principles of ISG. In this study, the principle of the hermeneutic circle was implied but explicit recognition was not given to it. As Klein and Myers (1999) found in the examination of the three sample articles that they evaluated, this lack of explicit recognition is due to the implication of the principle in the adherence to the other six principles.

The *principle of contextualization* was achieved through a clear and descriptive case study write-up. The history and context of the study was established upfront. The lack of security governance objectives was acknowledged and the organization's transition from current to new policies and controls was shared. The third principle, *interaction between the researchers and the subjects*, has been alluded to but not explicitly. One of the researchers spent more than six months with the organization. The level of trust between the researcher and the subjects increased during this period. The informal relationship with the

respondents helped in getting insights that contradicted what was being said by the participants. So the interaction of the researcher and subjects was such that good informal communication sessions were frequent. This relationship influenced the data collection and hence the findings of the study.

The *principle of abstraction and generalization* demands that idiographic details revealed by the data interpretation through the application of the principles one and two to theoretical concepts describe the nature of human understanding and social actions (Klein and Myers', 1999). This study was based on or guided by Value Theory. The guiding theory helped in understanding the importance of individual values in decision-making. Based on this premise, individual values about information security governance were elicited and converted into decision objectives.

The last three principles are about researcher's sensitivity in data analysis. The *principle of dialogical reasoning* indicates the researchers' sensitivity towards vetting possible contradictions between the theoretical preconceptions and the actual findings. In this study, Value theory is the intellectual basis. Some of the objectives were claimed to be important in interviews but were actually not being followed. These contradictions were noted and apparent reasons for these were discussed. Hence dialogical reasoning was performed and discussed. The *principle of multiple interpretations* demonstrates how the researcher shows sensitivity to differences in interpretations among the participants to the same event. The multiple perspectives of the top management, the middle management and the operational management on the same objectives actually led to better synthesis of the results and the ISG principles were created. Hence, this principle of multiple interpretations was used in

this research. Lastly *principle of suspicion*, recommends that the researcher should be sensitive to possible biases and distortions by the participants. In this research, the operational level people inserted distortions about the role of other agencies into the success of the security program. The top management believed that other agencies had minimal role to play in the success whereas others believed that due to politics, every step of the security policies and controls program would suffer delay.

7.4 Limitations

In this research or for interpretive field studies in general, there are two major areas of criticism- namely generalizability and researcher bias. A discussion on the generalizibility of the results is presented in chapter 3. In an interpretive field research, many of the findings do not hold true in other organizations. It is not the intention of this research to do so. The results are not generalizable in statistical sense but are generalizable to theory. The contributions in theoretical sense are presented in the previous section. Yin (2003) calls this analytic generalization which means theories used in other studies can be used as a template to compare the results.

Another criticism could be that the researcher as the research instrument allows several confounding variables to creep in, which bias the results. The objectivity of the case study was maintained by the researchers by restricting themselves to the objectives developed during phase 1. The researchers maintained distance from the data and remained focused on interpreting the case situation in the light of developed objectives. By consciously stating the historical and intellectual basis of this research and involving what the

interviewees said in critical reflections, we refrained from falling prey to bias and showed how the various interpretations emerged in this research (Klein and Myers 1999).

For data collection phase, we ensured that only individuals with substantial experience in using information technology with more than 5 years of managerial experience in relevant area were interviewed. Even though the interviewees appeared knowledgeable and concerned about governance issues, it is possible that their understanding about security governance is not a true representation of the actual state of affairs.

7.5 Future research directions

There are several streams of work that can arise from this research. Some of these are discussed below.

The list of objectives developed in this research can be subjected to psychometric analysis with separate large samples. Development of a model for measuring information security governance could result from such an exercise. This research is more exploratory in nature and uses qualitative data to test the validity of the objectives and establishing the relations for means-end framework. But the next obvious step would be test the model using quantitative data and perform confirmatory factor analysis. The models thus developed could be tested using structure equation modeling techniques.

Second, further investigation to establish relationships between means and fundamental objectives is required. Statistical tests could be performed for each of the paths suggested in the means-end framework developed, rather than basing the relationships merely on arguments.

Third, more investigation is required to assess the correlations of the means objectives within a fundamental objective and also correlations of the fundamental objectives themselves. This stream of work requires quantitative data and multivariate analytical techniques for analyzing the data.

Fourth, using multi objective decision analysis techniques, decision models can be created for organizations. These models can help prioritize resources invested for the objectives based on aggregate weights of the objectives and by ranking them in order.

Fifth, the objectives proposed in this research needs to be operationalized in order to be achievable and useful in day-to-day activities. Further research is required to develop activities and tasks for every objective so that the controls can be optimally designed.

References

Abouzakhar, N., and Manson, G. "An intelligent approach to prevent distributed systems attacks " Information Management & Computer Security (10:5) 2002, pp 203-209.

Adams, A., and Sasse, M.A. "Users are not the enemy. Association for Computing Machinery," Communications of the ACM (42:12) 1999, pp 40-46.

Albanese, R. "Criteria for Evaluating Authority Patterns," Academy of management Journal (16:1) 1973, pp 102-111.

Allen, J., and Westby, J.R. "Characteristics of Effective Security Governance ", Carnegie Mellon University, Software Engineering Institute, CERT®

Alves, G., Carmo, L., and Almeida, A. "Enterprise Security Governance: A practical guide to implement and control Information Security Governance " Business-Driven IT Management (BDIM) IEEE/IFIP International Workshop 2006, pp. 71-79.

Amer, S., and Hamilton, J. "Understanding Security Architecture," Proceedings of 2008 Spring simulation multiconference, ACM 2008.

Anderson, P.W. "Information Security Governance," pp. 60-70.

Anderson, E. and Choobineh, J. "Enterprise Information Security strategies," *Computers and Security*, 27(1), 2008, p. 22-29

Angell, I.O. "Systems thinking about information systems and strategies," Journal of Information Technology (5) 1990, pp 168-174.

Angell, I.O. "Ethics and Morality - a business opportunity for the Amoral?," Journal of Information System Security (3:1) 2007.

Anonymous "Spiritual Ethics and Information Security," Computer Fraud & Security), October 1997.

Anonymous "For security, First step is teamwork," Building Operating Management (53:3) 2006, pp 64-68.

Anthony, R., Dearden, J., and Bedford, N. Management Control Systems, Homewood, Irwin, 1989.

Anttila, J., Savola, R., Kajava, J., Lindfors, J., and Röning, J. "Control of agency problems in information security: Fulfilling the needs for information security awareness and learning in

information society " 6th Annual Security Conference, The Information Institute, USA Las Vegas, 2007.

AS/NZS 4360 (1999) `Risk Management' Standards Australia, 1995, 1999

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

Banks, D.G. "The fight against fraud," The Internal Auditor (61:2) 2004, pp 34-39.

Baskerville, R., and Siponen, M. "An information security meta-policy for emergent organizations," Logistics Information Management Science (15:5) 2002, pp 337-346.

Beath, C.M. "Supporting the Information Technology champion," MIS Quarterly), September 1991, pp 355-372.

Behling, C.S.a.R. "Developing and implementing a strategy for technology deployment " The Information Management Journal), July/August 2006, pp 52-57.

Bennet, V., and Cancilla, B. (2005). IT responses to Sarbanes-Oxley. *IBM*. Retrieved on 09/30/08 http://www-128.ibm.com/developerworks/rational/library/sep05/cancilla-bennet/index.html.

Betteridge, P. "Role-Based Access Control –a Real World Solution " Computer Fraud & Security:12) 2002, pp 9-11.

Birch, D., and McEvoy, N. "Risk analysis for information systems," Journal of Infomration Technology (7) 1992, pp 44-53.

Booker, Q., and Kitchens, F. "Predicting employee intention to comply with organizational security policies and procedures factoring risk perception " 5th Annual Security Conference, The Information Institute, USA, Las Vegas, 2006.

Booker, Q., and Kitchens, F. "Examining security intentions of multiple security measures " 7th Annual Security Conference The Information Institute, USA, Las Vegas, 2008.

Booker, R. "Re-engineering enterprise security," Computers & Security (25) 2006, pp 13-17.

Bresser, R., and Bishop, R. "Dysfunctional effects of formal planning: Two theoretical explanations," The Academy of Management Review (8:4) 1983, p 588.

Brown, W., and Nasuti, F. "Sarbanes-Oxley and Enterprise Security: IT Governance-What it Takes to Get," Information Systems Security (14:5) 2005, pp 15-28.

Burrell, W., and Morgan, G. Sociological Paradigms and Organizational Analysis Ashgate Publishing, Brookfield, VT, 1979.

Butler, J.K. "Toward understanding and measuring conditions of trust: Evolution of a condition of trust inventory," Journal of Management (17) 1991, pp 643-663.

Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G. and Mickunas, M. D "Towards Security and Privacy for Pervasive Computing. In Theories and Systems," in: Mext-NSF-JSPS International Symposium, ISSS, Tokyo, Japan, 2002.

Canal, V. "Usefulness of an Information Security Management Maturity Model " Information Systems Control Journal (2) 2008.

Catton, W.R. "Exploring Techniques for Measuring Human Values," American Sociological Review (19:1) 1954, pp 49-55.

Catton, W.R. "Propaganda Effectiveness As A Function Of Human Values," in: sociology, University of washington, 1954, pp. 1-196.

Catton, W.R. "A Retest of the Measurability of Certain Human Values," American Sociological Review (21:3) 1956, pp 357-359.

Catton, W.R. "A Theory of Value," American Sociological Review (24:3) 1959, pp 310-317.

Center, C.C.R. "Computer crime: Data breaches," 2006.

CERT "CERT/CC Statistics 1988-2006," CERT Coordination Center, 2006.

Chau, J. "Application security – it all starts from here," Computer Fraud & Security), June 2006.

Chin, A and Mishra, S. "Increasing Governmental Regulations and their impact on IT:SOX and HIPPA", Proceedings of International Resource Management Association conference, Washington D.C. 2006, May 17-20

Cohen, S. and Levinthal, D. "Absorptive Capacity: A new perspective on learning and innovation," *Administrative Science Quarterly*, 35, 1990, p. 128-152

COSO "Putting COSO theory into Practice: Tone at the Top," Committee of Sponsoring Organization of the Treadway Commission Retrieved on 10/10/08 www.coso.org

Coviello, A. and Swindle, O. "It's time to band together for better data security". *Computerworld*, January 2006. Retrieved on 05/05/06. http://www.computerworld.com/securitytopics/security/story/0,10801,107830,00.html)

Cummings, L. "Dear IT: Forget the technology," Network World (25:24) 2008, pp 34-35.

Davis, R. "The Philosophy of Management," Academy of management Journal) 1958, pp 37-40.

Deloitte "Global Security Survey," 2006. Retrieved on 09/10/08http://www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecuritysurvey(1).pdf

DeMaio, H. "Global trust, certification and (ISC)2 " Elsevier Science Ltd.,) 2002, pp 701-704.

Detmar W. Straub, R.J.W. "Coping with systems risk: security planning models for management decision making," MIS Quarterly), Decembers 1998, pp 441-469.

Dhillon, G. "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security 20(2): 165-172.," Computers & Security (20:2) 2001, pp 165 - 172

Dhillon, G. Principles of Information Systems Security: Text and Cases Wiley, 2006.

Dhillon, G., and Backhouse, J. "Information System Security Management in the New Millennium," Communications of the ACM (43:7) 2000, pp 125- 128.

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

Dhillon, G. and Mishra, S. "The Impact of Sarbanes-Oxley (SOX) Act on Information Security Governance" In *Enterprise information security assurance and system security: Managerial and technical issues*, Warkentin, M & Vaughan, R. (Eds.), Hershey, PA: Idea Group Publishing, 2006, pp. 62-79

Dhillon, G., and Moores, S. "Computer crimes: theorizing about the enemy within," Computers & Security (20:8) 2001, pp 715-723.

Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.

Dhillon, G. and L. Silva (2001). Interpreting computer-related crime at the Malaria Research Center: a case study. In Advances in information security management & small systems security. Eds. J. H. P. Eloff, L. Labuschagne, R. Solms and G. Dhillon. Boston, Kluwer Academic Publishers: 167-182.

Drazin, R., Glynn, M., and Kazanjian, R. "Multilevel theorizing about creativity in organizations: A sense making perspective " The Academy of Management Review (24:2), April 1999, pp 286-307.

Drevin, L., Kruger, H.A., and Steyn, T. "Value-focused assessment of ICT security awareness in an academic environment," Computers & Security (26) 2007, pp 36-43.

Drummond, H. "Did Nick Leeson have an accomplice ? The role of information technology in the collapse of Barings Bank," Journal of Information Technology (18) 2003, pp 93-101.

Dutta, A., and McCrohan, K. "Management's role in information security in a cyber economy " California Management Review (45:1) 2002, pp 67-87.

Eloff, J.H.P., and Eloff, M. "Integrated Information Security Architecture " Computer Fraud and Security (11) 2005, pp 10-16.

Eloff, M., and von Solms, S.H. "Information Security Management: An Approach to Combine Process Certification And Product Evaluation " Computers & Security (19) 2000, pp 698-709.

Essex, P and Schauer, P and . "Common sense security," Ohio CPA Journal (60:1), Jan - Mar 2001, pp 12-16.

Evan E. Anderson, J.C. "Enterprise information security strategies," Computers & Security) 2008, pp 22-29.

Ezingeard, J., McFadzean, E., and Birchall, D. "A Model of Information Assurance Benefits " Information Systems Management (22:2) 2005, p 20.

Farris, G. (2004). Mitigating the Ongoing Sarbanes-Oxley Compliance Process with Technical Enforcement of IT Controls. *DM Direct Newsletter*. DMReview.com

Finne, T. "The information security chain in a company " Computers & Security (15:4) 1996, pp 297-316.

Fleming, S. "Implicit Trust Can Lead to Data Loss," Information Systems Security (16) 2007, pp 109-113.

Flowerday, S., and Solms, R. "Real-time information integrity = system integrity+ data integrity +continuous assurances," Computers & Security (24) 2005, pp 604 - 613

Ford, C.M. "A theory of individual creative action in multiple social domains " The Academy of Management Review (21:4), October 1996, pp 1112-1142.

Forte, D., and Power, R. "Guaranteeing governance to curb fraud- Societe Generale debate " Computer Fraud & Security), March 2008, pp 18-19.

Fox, C. (2004). Sarbanes-Oxley- Considerations for a Framework for IT Financial Reporting Controls. *Information Systems Control Journal*, Vol. 1.

Fuller, C., Biros, D., and Imperial, M. "Knowledge retention in information assurance computer-based training: a comparative study of two courses for network user " 6th Annual Security Conference, The Information Institute, USA, Las Vegas, 2007.

Furnell, S. "E-commerce security a question of trust" Computer Fraud & Security:10) 2004, pp 10-14.

Galloway, D.J. "Control models in perspective," The Internal Auditor (51:6) 1994, pp 46-52.

GAISP, “Generally Accepted information Security Principles”, 2006. Retrieved on 10/10/07 www.gaisp.org

Garigue, R. and Stefaniu, M. “Information Security Magazine,” Information Security Magazine, 2004

Gioia, D., and Pitre, E. "Multiparadigm Perspectives on Theory Building," Academy of Management Review (15:4) 1990, pp 584-602.

Goel,S., Pon, D., and Manzies, J. "Managing information security: Demystifying the audit process for security officers " Journal of Information System Security) 2006, pp 25-45.

Gordon, S. "Technologically Enabled Crime: Shifting Paradigms for the Year 2000," Computers & Security (14) 1995, pp 391-402.

Gregor, S. "The Nature of Theory in Information Systems," MIS Quarterly (30:3) 2006, pp 611-642.

Guba, E., and Lincoln, Y. "Competing paradigms in qualitative research," in: Handbook of Qualitative Research, N. Denzin and Y. Lincoln (eds.), Sage, Thousand Oaks, CA, 1994, pp. 105-117.

Gupta, M., and Sharman, R. "Evaluating organizational social engineering threats: A metrics development framework " 7th Annual Security Conference The Information Institute, USA, Las Vegas 2008.

Haara, H., and Von Solms, R. "A Model for Deriving Information Security Control Attribute Profiles," Computers & Security (22:3) 2003, pp 233-244.

Hansen, J.V., and Hill, N.C. "Control Audit of Electronic Data Interchange," MIS Quarterly:4) 1989, pp 403-413.

Hanseth, O., Jacucci, E., Grisot, M., and Aanestad, M. "Reflexive Standardization: Side Effects and Complexity in Standard Making," MIS Quarterly (30 Special Issue/ August) 2006, pp 563-581.

Henderson, J.C., and Lee, S. "Managing I/S Design Teams: A Control Theoreis Perspective," Management Science (38:6) 1992, pp 757-777.

Henderson, J.C., and Venkatraman, N. "Strategic Alignment; A Model for Organizational Transformation Through Information Technology," in: Transformaing Organizations, T.A. Kochan and M. Useem (eds.), Oxford University Press, New York, 1992.

Henry, K. “This is your Life: How secure is your CRM Data?,” *Computer Fraud & Security*, September, 9, 2001, p. 10-11

Heschl, J. "CoBiT in Relation to Other International Standards," Infomration systems control journal (4) 2004.

Hinde, S. "Banking on security and control ?," Computer Fraud & Security:8) 2004, pp 4-6w.

Hinde, S. "Crime and punishment: corporate governance " Computer Fraud & Security:6) 2004, pp 4-6.

Hinde, S. "IT controls, financial reporting and fraud " Computer Fraud & Security:7) 2004, pp 13-15.

Hirschi, T. Causes of Delinquency Univerisity of California Press, Berkeley, CA, 1969.

Hogg, M., and Terry, D. "Social identity and self-categorization processes in organizational contexts," Academy of Management Review (25:1) 2000, pp 121-140.

Huberman, A., and Miles, M. "Data Management and Analysis Methods," in: Handbook of Qualitative Research, N. Denzin and Y. Lincoln (eds.), Sage, Thousand Oaks, CA, 1994, pp. 429-444.

IIA "Organizational Governance: Guidance for Internal Auditors," The Institute of Internal Auditors 2006, pp. 1-18.

ISACA "CISA Review Manual," Information Systems Audit and Control Association, Rolling Meadows, IL, 2004.

ISO "ISO/IEC 17799:2005," International Organization for Standardization 2005.

ITGI, and OGC "Aligning CobiT, ITIL and ISO 17799 for Business Benefit," Information Technology Governance Institute and Office of Governement Commerce, pp. 1-62.

ITGI (2003) IT Control Objectives for Sarbanes-Oxley. IT Governance Institute, Rolling Meadows

ITIL "ITIL V3," 2007. Retrieved on 10/10/08 http://www.itlibrary.org/

Jain, A., and Raja, M.K. "An exploratory assessment of security principles & practices: an insight from a financial services company " 6th Annual Security Conference, Information Institute Publishing, USA, Las Vegas, 2007.

Johnson, E.C. "Security awareness: switch to a better programme," in: Network Security 2006, pp. 15-18.

Johnson, R.A.H., Robert E; Hitt, Michael A "Board of director involvement in restructuring: The effects of board versus," Strategic Management Journal (14) 1993, pp 33-50.

Johnston, A., Eloff, J., and Labuschagne, L. "Security and human computer interfaces," Computers & Security (22:8) 2003, pp 675-684.

Jones, G., and George, J. "The experience and evolution of trust: Implications for cooperation and teamwork " The Academy of Management Review (23:3), July 1998, pp 531-546.

Kankanhallia, A., Teo, H., Tan, B., and Wei, K. "An Integrative Study of Information Systems Security Effectiveness," International Journal of Information Management (23) 2003, pp 139-154.

Karydaa, M., Kiountouzisa, E., Kokolakisb, S "Information systems security policies: a contextual perspective," Computers & Security (24) 2005, pp 246-260.

Keeney, R. Value-focussed thinking: a path to creative decisionmaking Harvard University Press, Cambridge:Massachusetts, 1992.

Keeney, R. "The Value of Internet Commerce to the Customer," Management Science (45:4) 1999, pp 533-542.

Kerry-Lynn Thomson and Rossouw von Solms, P.E.T. "Towards an information security competence maturity model " Computer Fraud & Security), May 2006, pp 11-15.

Kim, G. "Sarbanes-Oxley, fraud prevention, and IMCA: A framework for effective controls assurance " Computer Fraud & Security), pp 12-16.

Kirkwood, C.W. Strategic decision making: Multipbjective decision analysis with spreadsheets Duxbury Press, Belomont, CA, 1997.

Kirsch, L.J. "Deploying Common Systems Globally: The Dynamics of Control," Information Systems Research (15:4) 2004.

Kirsch, L.J., Sambamurthy, V., Ko, D.-G., and Purvis, R.L. "Controlling Information Systems Development Projects:The View from the Client " Management Science (48:4) 2002, pp 484-498.

Klein, H.J. "An Integrated Control Theory Model of Work Motivation," Academy of Management Review (14:2) 1989, pp 150-172.

Klein, H.K., and Myers, M. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems " MIS Quarterly (23:1) 1999, pp 67-93.

Knapp, K., Marshall, T., Rainer, R., and Ford, F. "Information security: management's effect on culture and policy," Information Management & Computer Security (14:1) 2006, pp 24-36.

Kolokotronis N, Margaritis C, Papadopoulou P, Kanellis P and Martakos D, " An Integrated Approach for Securing Electronic Transactions over the Web," *Benchmarking* 9(2), 166-181, 2002

Krull, A. "Whistleblowers and Informants, Part2 " Computer Fraud & Security), October 1996.

Lainhart IV, J. "An IT assurance framework for the future " Ohio CPA Journal (60:1) 2001, pp 19-23.

Lane, V.P. Security of Computer Based Information Systems Macmillan, London, 1985.

Lange, L. "Why ITIL Rules," 2007 Retrieved on 10/12/08 http://www.smartenterprisemag.com/articles/2007winter/bestpractices.jhtml

Langfield-Smith, K. "Management Control Systems and Strategy: A critical Review," Accounting. Organizations and Society (22:2) 1997, pp 207-232.

Leach, J. "Improving User Security Behavior," Computers & Security (22:8) 2003, pp 685-692.

Lee, A., and Baskerville, R. "Generalizing Generalizability in Information Systems Research," Information System Research (14:3) 2003, pp 221-243.

Lee, A.S. Thinking about Social theory and Philosophy for Information Systems John Wiley & Sons, Ltd, Chichester, England, 2004, pp. 1-26.

Lee , S., Lee, S.M., and Yoo, S. "An Integrative Model Of Computer Abuse Based On Social Control And General Deterrence Theories," Information and Management (41:6), July 2004 2004, pp 707-718.

Lepine, J., and Dyne, L. "Peer responses to low performers: An Attributional model of helping in the context of groups," Academy of Management Review (26:1) 2001, pp 67-84.

Leyden, J. "Human error blamed for most security breaches," in: The Register, 2004.

Lindup, K. "The Role of Information Security in Corporate Governance," Computers & Security (15) 1996, pp 477-485.

Liu, Q., and Ridley, G. "IT Control in the Australian public sector: an international comparison," Thirteenth European Conference on Information Systems, Regensburg, Germany, 2005.

Loch, K., and Conger, S. " Evaluating Ethical Decision Making and Computer Use," Communications of the ACM (39:7), July 1996 1996, pp 74-83.

Magklaras, G., and Furnell, S. "A preliminary model of end user sophistication for insider threat prediction in IT systems," Computers & Security (24) 2005, pp 371-380.

Marginson, D. “Management control systems and their effects on strategy formation at middle management levels: Evidence from a U.K organization,” *Strategic Management Journal*, 2002, 23(11), p. 1019

Marks, M., Mathieu, J., and Zaccaro, S. "A temporally based framework and taxonomy of team processes," Academy of management review (26:3) 2001, p 356.

Marks, N. "Another Voice on Controls," The Internal Auditor (62:3), June 2005, p 92.

May, C. "Dynamic corporate culture lies at the heart of effective security strategy," Computer Fraud & Security:5) 2003, pp 10-13.

Maynard, S.B., and Ruighaver, A.B. "Security policy quality: a multiple constituency perspective " 6th Annual Security Conference, The Information Institute, USA, Las Vegas, 2007.

McCarthy, M.P., and Campbell, S. Security Transformation McGraw-Hill, New York, 2001.

McFadzean, E., Ezingeard, J., and Birchall, D. "Anchoring Information Security Sociological Groundings and Future Directions," Journal of Information System Security (2:3) 2006.

McGuire, D., Garavan, T., Saha, S., and O'Donnell, D. "The impact of individual values on human resource decision-making by line-managers," International Journal of Manpower (27:3) 2006, pp 251-273.

McHugh, J., and Deek, F. "An incentive system for reducing Malware Attacks," Communications of the ACM (48:6), June 2005 2005, pp 94-99.

Melling, W. "Enterprise Information Architectures —They’re Finally Changing," SiGMOD 94, Minneapolis, Minnesota, USA 1994.

Mellor, M., and Noyes, D. "Awareness and accountability in information security training " 6th Annual Security conference The Information Institute, USA Las Vegas, 2007.

Merrick, J. and Garcia, M. “Using Value-Focused Thinking to Improve Watersheds,” *Journal of American Planning Association*, Summer 2004, 70(3), p. 313

Moulton, R., and Coles, R. "Applying Information Security Governance," Computers & Security (22:7) 2003, pp 580-584.

Mowday, R., and Sutton, R. "Organisational behavior: Linking individuals and groups to organisational contexts," Annual Review of Psychology (44) 1993, pp 195-230.

Myler, E. and Broadbent, G. "ISO 17799 : Standard for security " The Information Management Journal, November/December 2006, pp 43-52.

Neil F. Doherty, H.F. "Aligning the information security policy with the starategic information system plan " Computers & Security) 2006, pp 55-63.

NIST "Special Publication 800-53, Revision 2, " NIST (ed.), 2007, p. 188.

Orlikowski, W. "Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology," Accounting, Management and Information Technologies (1:1) 1991, pp 9-42.

Ouchi, W.G. "The Relationship between Organizational Structure and Organizational Control," Administrative Science Quarterly (22:1) 1977, pp 95-113.

Ouchi, W.G. "The Transmission of Control Through Organizational Hierarchy," Academy of management Journal (21:2) 1978, pp 173-192.

Ouchi, W.G. "A Conceptual Framework for the Design of Organizational Control Mechanisms," Management Science (25:9) 1979, pp 833-848.

Ouchi, W.G. "Markets, Bureacracies and Clan," Administrative Science Quarterly (25:1) 1980, pp 129-141.

Ouchi, W.G., and Maguire, M.A. "Organizational Control: Two Functions," Administrative Science Quarterly (20) 1975, pp 559-569.

Packard, H. "The HP Security Handbook," pp. 1-208.

Parker, D.B. "Information security controls for an organization undergoing radical changes," Information Systems Security (5:3) 1996.

Parnell, G., Conley, H., Jackson, J., Lehmkuhl, l and Andrew, J. “A framework for evaluating future air and space forces,” *Management Science*, 44(10), 1998, p. 1336-1350

Peppard, J., and Ward, J. "Beyond strategic information systems: toward an IS capability," Strategic Information Systems (13) 2004, pp 167-194.

Perry, W., and Warner, H.C. "A Quantitative Assessment Of Internal Controls," The Internal Auditor (62:2), April 2005, p 51.

Perry, W.E. "Developing a computer security and control strategy " Computers & Security) 1982, pp 17-26.

Peterson, R.B. "A Call for Testing Our Assumptions:Human Resource Management Today," Journal Of Management Inquiry (13:3), September 2004, pp 192-202.

Peterson, Z. and Burns, R. (2005). Ext3cow: A Time-Shifting File System for Regulatory Compliance. *ACM Transactions on Storage*. Vol. 1, No. 2 (190-212).

Philip, P.L., and Jonathan, K.H. "Risk management for information systems development," Journal of Information Technology (11) 1996, pp 309 - 319

Pierce, J.L., Kostova, T., and Dirks, K.T. "Towards A Thoery of Pschological Ownership in Organizations," Academy of Management Review (26:2) 2001, pp 298-310.

Poole, V. "Why Information Security Governance Is Critical to Wider Corporate Governance Demands—A European Perspective " in: Information Systems Control Journal, 2006.

Poore, R.S. "Information Security Governance " EDPACS (33:5) 2005, pp 1-7.

Posthumus, A., and Von Solms, R. " A framework for the governance of information security," Computers & Security (23) 2004, pp 638-646.

PriceWaterhouseCoopers "The Global State of Information Security,") 2006.

Privacy Rights Clearinghouse. "A Chronology of Data Breaches Reported Since the ChoicePoint Incident", 2006 Retrieved on 04/26/08.
http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

Qiang, Y and Hua-ying, S, "A Systematic Research and Simulation of the Internet Security Governance," Proceedings of ISTAS 2007, IEEE International Symposium on Technology and Society, 2007.

Ramos, M. "Evaluate the Control Environment," Journal of Accountancy (197:5, May 2004, p 75.

Ratnasingham, P, "Implicit Trust in the Risk Assessment Process of EDI," Computers and Security, 18(4), 1999, p. 317-321

Rees J, Bandyopadhyay S and Spafford, "PFIRES: A Policy Framework for Information Security, *Communications of the ACM* July 2003/Vol.46 (7) pp 101-106., 2003

Rezmierski, V.E., Seese, M.R., and St. Clair II, N. " University systems security logging: who is doing it and how far can they go? ," Computers & Security (21:6) 2002, pp 557-564.

Ridley, G., Young, J., and Carroll, P. "COBIT and its Utilization:A framework from the literture," 37th Hawaii International Conference on System Sciences IEEE, Hawaii, 2004.

Roger C. Mayer, J.H.D., F. David Schoorman "An Integrative model of organization trust " The Academy of Management Review (20:3), July 1995, pp 709-734.

Rokeach, M. *The nature of Human Values.*1973, Free Press, New York.

Rossouw von Solmsa, S.H.B.v.S. "Information Security Governance: A model based on the Direct–Control Cycle," Computer & Security (25) 2006, pp 408-412.

Ruighaver, A.B., Maynard, S.B., and Chang, S. "Organizational security culture: Extending the end-user perspective " Computers & Security (26) 2007, pp 56-62.

Rutgers Identity Theft Center. “Security Breach at Social Services in LA County”, 2006 Retrieved on 04/26/08 http://www.identitytheft911-sunj.com/alerts/alert.ext?sp=361

Ryana, J., and Ryanb, D. "Expected benefits of information security investments," Computers & Security (25) 2006, pp 5 7 9 – 5 8 8

S. Flowerday, A.W.B., R. Von Solms "Continuous auditing technologies and models: A discussion," Computers & Security) 2006, pp 325-331.

Saint-Germain, R. "Information Security Management Best Practice Based on ISO/IEC 17799," The Information Management Journal), July/August 2005, pp 60-66.

Sanders, W., and Carpenter, M. "Internationalization and firm governance: The roles of CEO compensation, top team composition, and Board structure " The Academy of Management Journal (41:2), April 1998, pp 158-178.

Sandhu, R., and Samrati, P. "Access Control: Principles and Practice," IEEE communications) 1994, pp 40-48.

Schein, E.H. Organizational Culture and Leadership Jossey-Bass, San Francisco, CA, 1992.

Schauer, P. "Common sense security," Ohio CPA Journal (60:1), January 2001, pp 12-16.

Schultz, E. "A framework for understanding and predicting insider attacks," in: Compsec London, 2002.

Schulz, M. "The uncertain relevance of newness: Organizational learning and knowledge flows " The Academy of Management Journal (44:4), August 2001, pp 661-681.

Schwartz, R. "Make Risk Management And Internal Controlwork For You," Strategic Finance) 2006, pp 35-42.

Scott, A. "ITGI Issues Control Guidance," The Internal Auditor (60:6), December 2003, p 15.

Scott, R.R. "Attribution of Internal Control," Journal of Black Studies (6:3) 1976, pp 277-290.

Scott, W.R. Organizations: Rational, Natural and Open Systems Prentice-Hall, Eaglewood Cliffs:N.J, 2005.

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

Senger, J. "Managers' Perception of Subordinates' Competence As a Function of Personal Value Orientation," Academy of management Journal) 1971, pp 415-423.

Shedden, P., Ruighaver, T., and Ahmed, A. "Risk management standards: The perception of ease of use," 5th Annual Security Conference, The Information Institute, USA, Las Vegas, 2006.

Sheng, H., Nah, F., and Siau, K. "Strategic implications of mobile technology: A case study using Value-Focused Thinking " Journal of Strategic Information Systems (14) 2005, pp 269-290.

Sherwood, J. "SALSA: A method for developing the enterprise security architecture and strategy " Computers & Security (15:6) 1996, pp 501-506.

Sia, S., and Neo, B. "Reengineering effectiveness and the redesign of organizational control," Journal of Management Information Systems (14:1) 1997, p 69.

Simons, R. "How new top managers use control systems as levers of strategic renewal," Strategic Management Journal (15:3), March 1994, p 169.

Smith, P.W.a.C.L. "The Development of Access Control Policies for Information Technology Systems," Computers & Security (21:4) 2002, pp 356-371.

Snell, S.A. "Control Theory in Strategic Human Resource Management: The Mediating Effect of Administrative Information," Academy of management Journal (35:2) 1992, pp 292-327.

Solms, B.v. "Information Security governance: COBIT or ISO 17799 or both?," Computers & Security (24) 2005, pp 99-104.

Solms, B.v. "Information Security-The Fourth Wave," Computers & Security (25) 2006, pp 165-168.

Solms, S.P.a.R.v. "IT oversight: an important function of corporate governance " Computer Fraud & Security), June 2005, pp 11-17.

Stanton, J., and Stam, K. "Analysis of end user security behaviors," Computers & Security (24) 2005, pp 124-133.

Stefaniu, R. and Garigue.M. "Information system governance reporting," Information System Security), September/October 2003, pp 36-40.

Steven De Haes , and Grembergen, W.V. "Analysing the Relationship Between IT Governance and Business/IT Alignment Maturity," 41st Hawaii International Conference on System Sciences, 2008.

Stoupa, K., and Vakali, A. "Clustering subjects in a credential-based access control framework " Computers & Security (26:2) 2007, pp 120-129.

Straub, D. "Coping with systems risk: security planning models for management decision making.," MIS Quarterly (22:8) 1998, pp 441-465.

Straub, D.W., and Welke, R.J. "Coping With Systems Risks: Security Planning Models for Management Decision Making," MIS Quarterly (22:4) 1998, pp 441-469.

Swanson, M. and Guttman, B. “Generally Accepted Principles for Securing Information Technology Systems,” National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1996

Tacconi, L. "Dissent from choice theory: implications for environmental decision making " International Journal of Social Economics (23:4) 1996, pp 331-345.

Tannenbaum, A. Control in Organizations McGraw-Hill, New York, 1968.

Taylor, R.G. "Management Perception Of Unintentional Information Security Risks," Twenty-Seventh International Conference on Information Systems, Milwaukee, 2006.

Tsiakis, T. and Sthephanides, G. "The concept of security and trust electronic payments " Computers & Security) 2005, pp 10-15.

Theoharidou, M., S. Kokolakis "The insider threat to information systems and the effectiveness of ISO17799," Computers & Security (24) 2005, pp 472-484

Thomson, K., and Von Solms, R. "Information security obedience: a definition," Computers & Security. (24:69-75) 2005.

Tickle, I. "Data integrity assurance in a layered security strategy " Computer Fraud & Security), pp 9-13.

Travis D. Breaux, A.I.A., Eugene H. Spafford "A distributed requirements management framework for legal compliance and accountability " Computers & Security) 2008, pp 1-10.

Trček, D. "An integral framework for information systems security management," Computer & Security (22:4) 2003, pp 337-360.

Trompeter, C., and Eloff, J. "A Framework for the Implementation of Socio-ethical Controls in Information Security," Computers & Security (20:5) 2001, pp 384-391.

Truex, D.P., Baskerville, R., and Klein, H.K. "Growing Systems in an Emergent Organization," Communications of The ACM (42:8) 1999, pp 117-123.

Tudor, J.K. Information Security Architecture-An integrated approach to security in an organization Auerbach, Boca Raton, Fl, 2000.

Vaeiga, A.D., and Eloff, J.H.P. "An Information Security Governance Framework," Information Systems Management (24:4) 2007, pp 361-371.

Venkatraman, N., Henderson, J., and Oldach, S. "Continuous strategic alignment: exploiting information technology capabilities for competitive success.," European Management Journal (11:2) 1993, pp 139-149.

Violino, B. "Expect Threats to get nastier as networks become more complex," in: Computerworld, 2006.

Volonino, L., Kermis, G., and Gessner, G. (2004). Sarbanes-Oxley links IT to corporate compliance. In *Proceedings of the Tenth Americas Conference on Information Systems*. New York:

Von Solms, B. "Corporate Governance and Information Security," Computers & Security (20:3) 2001, pp 215-218.

Von Solms, B. "Information Security–A Multidimensional Discipline " Computers & Security (20) 2001, pp 504-508.

Von Solms, B., and Von Solms, R. " From Information Security to…Business Security?," Computers & Security (24) 2005, pp 271-273.

Von Solms, R., and von Solms, S.H. "Information Security Governance: A model based on the Direct-Control Cycle," Computers & Security (25) 2006, pp 408-412.

Vroom, C., and Von Solms, R. "Towards information security behavioral compliance.," Computers & Security (23:191-198) 2004.

Wagner, J.K. "Leading the Way," The Internal Auditor (57:4) 2000, pp 34-39.

Walsham, G. Interpreting Information Systems in Organizations Wiley, Chichester, UK, 1993.

Walsham, G. "The Emergence of Interpretivism in IS Research," Information System Research (6:4) 1995, pp 376-394.

Walsham, G. "Doing Interpretive Research," European Journal of Information Systems (15:3) 2006, pp 320-330.

Walters, M. "A Draft of an Information Systems Security and Control Course," JOURNAL OF INFORMATION SYSTEMS (21:1) 2007, pp 123-148.

Ward, J., and Peppard, J. Strategic Planning for Information Systems John Wiley & Sons Ltd, Baffins Lane, Chichester, 2002.

Ward, P., and Smith, C. "The Development of Access Control Policies for Information Technology Systems," Computers & Security (21:4) 2002, pp 356-371.

Warkentin, M., and Johnston, A. IT Security Governance and Centralized Security Controls Idea Group Publishing, Hershey, P.A, 2006.

Warman, A.R. "Organizational computer security policy: the reality," European Journal of Information Systems (1:5) 1992, pp 305-310.

Webb, P., Pollard, C., and Ridley, G. "Attempting to Define IT Governance: Wisdom and Folly?," 39th Hawaii International Conference on Systems Sciences Hawaii, 2006.

Weber, R. Ontological Foundations of Information Systems Coopers & Lybrand, Australia, 1997.

Whitley, J. "Report Stresses Security Governance " The Internal Auditor (62:5) 2005, p 16.

Whitman, M. "Enemy at the Gate: Threats to Information Security," Communications of the ACM (46:8) 2003, pp 91-95.

Whitman, M., Townsend, A., and Aalberts, R. "Information Systems Security and the Need for Policy," in: Information Security Management: Global Challenges in the New Millennium., G. Dhillion (ed.), IGI Global, 2001, pp. 9-18.

Williamson, O.E. Markets and Hierarchies: Analysis and Antitrust Implications Free Press, New York, 1975, p. 286.

Wilson, P. "Risk control: a technical view," Computer Fraud & Security) 2005, pp 8-10.

Wilson, P. "Governance and security: side by side," Computer Fraud & Security) 2007.

Wing, S. "The importance of incorporating security requirements within system architecture rather than incorporating retro fitting controls to an insecure design " Computer Fraud & Security), 12-15 2006, p October.

Wood, C.C. "Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature " Computer Fraud & Security:1) 2004, pp 16-17.

Wright, M.A. "Keeping top management focused on security " Computer Fraud & Security (5:1) 2001, pp 12-14.

Xiu-Zhen Chena, Q.-H.Z., Xiao-Hong Guana, Chen-Guang Lina, Jie Sun "Multiple behavior information fusion based quantitative threat evaluation," Computers & Security (24) 2005, pp 218-231.

Yin, R. Case Study Research: Design and Methods Sage, Newbury Park, CA, 2003.Yugay, I. and Klimchenko, V. (2004). SOX Mandate Focus on Data Quality and Integration. *DM Review Magazine*. Dmreview.com Retrieved on 09/30/05

APPENDIX

Interview Template for the study

The interview will start with a discussion on informed consent. The researcher will read the attached consent form and explain in length about the consent form before the interview begins. The interviewee will sign the consent form before being interviewed.

List of guiding Questions

1. What are your values about internal controls for information systems security? By values we mean things that you feel are important and should be reflected in the controls.

2. Please elaborate what things are important to you for control design with examples/stories/experience.

3. Why are these things important to you in context of internal control design? Do you think these things make more secure information systems? How so? Elaborate.

4. In an ideal situation, when you have to design internal controls for information systems security in an organization from scratch, what are the things you will like to include and why?

5. Why do you think some of the controls work or do not work? Elaborate.

6. How important is it, in your opinion, to incorporate the feedback of employees about such controls and why? Elaborate.

7. There are many regulatory compliance issues forcing organizations to make changes in their control structure. Does compliance drive internal control design in your organization? How much? Explain.

8. How important is it, in your opinion, to communicate the intent of such controls to employees? Does it make any difference in your opinion? How so? Explain.

Interview Template for the second phase of the study

The interview will start with a discussion on informed consent. The researcher will read the attached consent form and explain in length about the consent form before the interview begins. The interviewee will sign the consent form before being interviewed.

List of guiding Questions

1. What are your values about internal controls for information systems security? By values we mean things that you feel are important and should be reflected in the controls.

2. Please elaborate what things are important to you for control design with examples/stories/experience.

3. Why are these things important to you in context of internal control design? Do you think these things make more secure information systems? How so? Elaborate.

4. How important is regulatory compliance plan in your organization? Does is help the internal control structure in organization? Explain

5. How can you improve the control implementation process? Elaborate.

6. How important is it, in your opinion, to incorporate the feedback of employees about such controls and why? Elaborate.

7. How important is it to establish deterrence criteria for the employees? Can you share any experience where lack of deterrence proved to be harmful for the organization?

8. How important is it, in your opinion, to communicate the intent of such controls to employees? Does it make any difference in your opinion? How so? Explain.

9. What proactive controls initiatives are important to assure successful control development and implementation? Explain with examples

10. In your opinion, is it helpful to have visible leadership for effective security controls? Why or why not?

11. Does clear responsibility and accountability in structures help in implementing security controls effectively? Explain

12. How does clarity in processes help in instituting controls? Explain

13. Do you think audit helps in developing better control structure? Explain with examples

14. Do you think clarity in controls can be achieved through effective communications and training about the subject? Why or why not?

15. Is it important to have a control strategy? Does separate control assessment functionality help in control implementation? Explain

16. Is the culture in your organization help in understanding the importance of security controls? How so?

17. Is the management involved in the controls development process? Is it helpful to get the management involved? Why or why not?

18. Does your organization attempts to standardize the controls? Does it help? Explain

Interview Log for Phase1 of the study

Respondent	Industry	Role	Duration (minutes)
1.	Healthcare	IT Director	35
2.	Credit card services	Security Manager	50
3.	Insurance	Security Officer	40
4.	Telecommunications	IT Director	60
5.	Telecommunications	Helpdesk IT specialist	30 (P)
6.	Telecommunications	Manager-HR	55
7.	Credit card services	IT Director	20
8.	Telecommunications	Manager-Accounts	70
9.	Insurance	Security Manager	25
10.	Energy	Helpdesk IT specialist	60
11.	Energy	IT Director	47
12.	Insurance	Helpdesk IT specialist	20
13.	Credit card services	Security Officer	25
14.	Credit card services	Manager-Accounts	10
15.	Insurance	Security Officer	80
16.	Telecommunications	Security Manager	90
17.	Credit card services	Systems Auditor	80
18.	Healthcare	System Administrator	80
19.	Internet service providers	Systems Auditor	25
20.	Credit card services	Manager-Finance	15
21.	State agency	IT Director	40
22.	State agency	CIO	60
23.	Insurance	Systems Auditor	60
24.	Insurance	Manager-Administration	25
25.	Insurance	Manager-HR	45 (P)

Respondent	Industry	Role	Duration (minutes)
26.	Health services	IT Director	50
27.	Health services	CEO	15
28.	Health services	Systems Auditor	30
29.	Internet service providers	Manager-HR	35
30.	Internet service providers	Security Manager	50
31.	Financial investment	Manager-Accounts	25
32.	Credit card services	Systems Auditor	30
33.	Internet service providers	System Administrator	40
34.	Credit card services	Systems Auditor	50
35.	Internet service providers	Helpdesk IT specialist	20
36.	Banks	System Administrator	45
37.	Banks	Manager-Administration	30
38.	Real estate development	Security Manager	15
39.	Financial investment	Security Officer	30
40.	Financial investment	Security Officer	45
41.	Real estate development	System Administrator	60

Interview log for phase 2: CCIT

Respondents	Roles	Duration (minutes)
1.	Chief Information Officer	60 60 (repeat)
2.	Security Director	45 30 (repeat)
3.	Security Manager	45 40 (repeat)
4.	Security Officer	40
5.	IT Development-Manager	50
6.	IT infrastructure-Manager	50
7.	Administration-Manager	60
8.	Help desk IT staff 1	30
9.	Help desk IT staff 2	30
10.	Internal Audit Director	60
11.	Internal Audit Officer	50 40 (repeat)
12.	Project Management-Manager	45

Table: Raw Values-Common Form Values-041008

Maximize Information Security Governance

No.	Raw Values	Common Form Values
1.	Problems you come across are usually lack of awareness about controls	**Lack of awareness is a source of problems for controls.**
2.	With media hype and everything with respect to governance failure .. security is becoming very important for business.	**Responsiveness to media hype**
3.	Awareness and responsibility for your action ..know what you are doing	**Clarity of responsibility in organizations Accountability for actions**
4.	using some of your knowledge in daily practices and in dealing with organizational issues	**Leverage individual knowledge for ensuring internal controls**
5.	pretty much be aware of what people should do and should not do	**Ensure awareness of organizational actions and practices**
6.	training implemented in such a way that .. you not only develop the principle of security or privacy but also let them know what are the common uses of it …here you should be using them...	**Training should reflect principles of internal controls rather than means of ensuring security**
7.	social engineering, you have to watch out before you say any thing make sure they identify them self correctly.	**Increase awareness of internal control breaches through social engineering**
8.	contract employee are asked to reset password every month	**Define policies for access to information resources**
9.	making sure no single point if failure , unfortunately you have to remember more than one password for this	**Define multiple layers of controls**
10.	we do have some feedback from various people ... not everything is convenient but people are getting used to it.. There is no other option	**Define a system for incorporating feedback to improve controls Balance convenience with usability**
11.	controls are in the policy in order to impose the policy (meaning - ensure compliance – as interpreted by the researcher via probes)	**Ensure compliance with internal controls defined in the policy document**
12.	We all tend to bring along.. some of the experiences… it may not be… the way we put it one the table	**Individuals differences in managing internal controls**
13.	designed our audit program overtime we changed .. so we are still undergoing additional tuning..	**Internal audit control practices need to evolve with time and changing contexts**
14.	Certainly we take input from auditees. It's the part of the process	**Take input from various individuals dealing with controls on a day to day basis**
15.	Usually there couple of points of contact … who help coordinate our efforts and help in audit.. and those POC provides us with other point of contact	**Auditing and compliance with controls is also based on informal feedback from trusted informants**
~~16.~~	~~we sit down with these people we have this one on one with them…~~	~~**Sit with people individually and take their perspective on the process**~~

17.	we might go back to the procedure and .. tell them what Joe told me… so they may fail on their own procedure…	**Internal control audit involves cross checking procedures with people**
18.	people who are really knowledgeable and know what they are doing ….-but hey haven't be able to push what they have been doing … because of the resources tie	**Individuals have ability to improve internal controls.** **Individuals constrained because of resource allocations**
19.	Generally speaking auditors think of themselves as…. I think they are somewhat of consultants…	**Internal control auditors are indeed consultants who ensure effectiveness of controls**
20.	some times controls fall through the crack.. they might be initially good controls but fail with change	**Internal control structures are not static. Proper change management needed for efficacy of controls**
~~21.~~	~~he has right access.. and the role changes and all changes~~ TASK	~~**Controls should consider change of roles**~~
~~22.~~	~~we do not create controls.. we only test them.. we consult about them …~~ TASK	~~**Controls need to be tested appropriately**~~ ~~**Controls are created by the management and employees**~~
~~23.~~	~~the appropriateness of access…and that's very high level generic controls… the specific which show appropriateness of access… the specific tool you may use very different.~~ TASK	~~**High level controls are needed for direction**~~ ~~**Specific controls use different approaches by organizations**~~
~~24.~~	~~the organization restructure… what controls do you have to make sure you changes your procedure accordingly.. or do the procedures need to be changed~~	~~**Change management controls are important**~~
25.	The application should not be a black box (interpretation – clarity of processes). We should understand the processes.	**Clarity of business processes for internal controls**
26.	if you just even go to policies… and try to implement the control so that you can answers some of the question, you will be far ahead….	**Encourage discussion on internal controls as identified in the policies**
27.	COBIT… gets some experts on COBIT.. It is pretty big model very generic. It teaches you to think about what you have to think about…	**Be aware of industry frameworks and models.** **They guide proper internal control formulation.**
~~28.~~	~~Look at COBIT and try to follow COBIT… you may need lot of interpretation…it going to be a long process…. Companies have separate COBIT implementation project..~~	~~**Generic frameworks need interpretation**~~ ~~**Following industry frameworks requires preparations**~~
29.	They have taken over all the localized controls and centralized access controls…	**Balancing centralization vs decentralization (move to 9)**
30.	You can't say it's not our fault because it's your yard…. If you feel that you should have way of knowing that..	**Consequences of internal control breaches should be communicated. (move to under 3 above)**
31.	regulatory compliance drives a lot what we do	**Encourage regulatory compliance to internal controls**
32.	Control consciousness came because of regulatory compliance.	**Establish a control consciousness culture** **Establish a compliance culture**

~~33.~~	~~Auditing became more important~~	~~**Auditing has gained importance as a functionality**~~
34.	SOX is way too strong we might have to step down	**Regulations may be too strong to be followed in entirety – define appropriate internal controls in response to regulations**
~~35.~~	~~We have everything SOX talks about already build in just matter of depth. SOX helps get us there quicker…~~	~~**Regulations help in following the controls better**~~
36.	It helped a lot in a popularity of controls.. people are scared of SOX	**Failure to comply with internal control regulations scares people**
~~37.~~	~~Repeat compliance is a bigger pain.~~	~~**Repeat compliance with regulations is difficult**~~
38.	Resources should be classified…. Regarding its sensitivity whether it is a proprietary information	**Internal control structures should reflect sensitivity of data**
~~39.~~	~~Access to those data resources…. should be restricted~~	~~**Access to data resources should be restricted**~~
40.	Authorization which should come from data owner	**Identify data owners for sensitive data** **Authorizations should be linked to data owners**
41.	access controls needs to be self protected	**Encourage individual responsibility for ensuring proper access to data resources.**
42.	Security controls needs to be driven from top of the organization to the bottom	**Top management involvement in defining internal controls for security**
43.	They set the tone for the entire organization…	**Top management should lead by example when dealing with internal controls**
~~44.~~	~~Executive should be aware in compliance era~~	~~**Awareness of compliance issues is important**~~
~~45.~~	~~most important thing is the direction from above.. management supports security incentives~~	~~**Direction should be provided from the top management**~~
46.	proper design of security.. ownership.. Authority.. privileges and roles… are clearly defined…. as well as the data resources…. With their sensitivity	**Role and privileges need to be properly defined and documented** ~~**Data resources should be clearly classified according to sensitivity level**~~
47.	most important thing is communicating that… to the individuals… an explanation to the individual about why	**Communication about the nature and scope of controls is important**
48.	Education is extremely important…	**Education of employees regarding internal controls is needed**
~~49.~~	~~the biggest impact from the facts that executive level… are being held accountable… for what there organizations are doing… if the rules were not followed~~	~~**Executives should be accountable for the actions**~~ ~~**Rules should be followed**~~
50.	when you change executive level change towards security .. you will absolutely change	**Change attitude of executives about security controls**

	organization attitude for security….	**Executives impact the organization's attitude towards security**
51.	Security is one key internal control…	**Security requirements define internal controls**
52.	Everybody got a security policy…and how well you keep them update. Communicate them.. maintain them or central to your security effort.	**Continuously update internal control requirements in security policies**
~~53.~~	~~Education as a control is probably…. is second most important thing in security.~~	~~**Education is an important control for security**~~
54.	controls over what people think are good.. usually starts with people… it need not be technology side.	**Controls need to be people oriented. Need to understand feelings, attitudes and belief of people.**
~~55.~~	~~security awareness training is good for control…~~	~~**Security awareness training is important for good controls**~~
56.	call security architecture review.. for anything goes into the production.	**Engage in an IT architecture review, which helps in correctness of design** **All program codes should be adequately reviewed**
57.	Part of our change management process is security.. architecture review.. which application developers.. …purchasing officials.. this meets security guidelines… and its another example of controls	~~**Change management process is important**~~ **All guidelines for governance need to be defined by consensus**
~~58.~~	~~Other controls ,in term of change management that we do.~~	~~**Change management should be adequately emphasized**~~
59.	The perspective is to ask questions about controls.. ask questions	**Relevance of all controls needs to be adequately discussed**
60.	Security controls are built along the way… such that the business can run smoothly..	**Controls in business processes are not an after-thought, they are designed and built as part of a change initiative**
61.	Nothing can derail a security initiative and change management quicker than agitating employees ..	**Do not agitate employees**
62.	for taking control away from people.. trying to impose…make people jump there hoops…	**Sudden changes in responsibility structures are not good for security governance** **Do not impose new rules on employees without careful consideration and proper buy-in**
63.	making sure people understand the priority understand roles , responsibility .. if you can demonstrate you can get the level of service	~~**Demonstrate clearly roles and responsibilities**~~ **Organizational members need to understand that certain tasks, controls and actions have a priority**
64.	some of the technology that support us .. such as audit tools.. should be run by separate groups…. Not run by security administrators…	**Auditing functions and actions need to be separated**

65.	having the control built in the low level are important.. Identity management… set of technology.. very important for controls for security management program	**Controls need to be at all levels of the organization – higher levels as well as lower levels** **Identity management is perhaps the most important control in organizations**
66.	external audit is another good stuff …	**Controls need to be periodically evaluated by external auditors**
67.	it becomes issue of internal policies…. it has to be related to IT architecture… client side you have to incorporate controls as part of system design…	**Controls should be related to the IT architecture** **Controls need to be instituted as part of organizational design**
68.	so for control point you need few people dedicated to doing this thing….. program management office .. project management…. Set of a separate office looking of security only	**There needs to be a management function that ensures efficacy of controls** ~~**Separate office is required for maintenance**~~
69.	it is a huge undertaking that goes back to identity management… we have so many environment to maintain.. we need tools for that.. .. the tools are very expensive	**The nature of controls determines that kind of tools necessary for management** **Resources need to be allocated for maintaining controls**
70.	.controlling people from inside is more of accountability and responsibility you have to make very clear the consequences of the action….	~~**Accountability and responsibility is required**~~ **Consequences of non compliance to controls needs to be communicated to the employees**
71.	But what is the criminal action… people are held responsible as the induction process begin in the company… but it's not clear if this happens.. what action would be taken …	**Explain the meaning of criminal action to the employees** ~~**Explain the consequences of action**~~
72.	security has to be a part of functional requirements…	**Security governance has to be a functional requirement**
~~73.~~	~~I believe we must make sure companies do the right thing. One way to accomplish this is through training.~~	~~**Ensure that companies do the right thing**~~ ~~**Training is required to help organizations do the right thing**~~
74.	Bridge the gap. MIS and Accounting have to play in the same sandbox.	**Bridge the gap between different functionalities in the organization** **MIS and accounting have to coordinate for better controls**
75.	Provide more training to MIS people. They need to understand the need for compliance.	~~**Provide training to technology oriented people such that they are responsive for compliance purposes**~~

		Explain the importance and need for compliance to technical people
76.	Changes in the corporate culture have to be managed in a better way.	**~~Better change management practices in the organization~~** **Appreciation for cultural aspects needs to be central in organizing security governance controls**
77.	nly people are reviewing everything that you do…such changes have to be managed properly.	**Review of controls should be in light of the organizational objectives**
78.	Security governance should be a way to move forward to, build the new program into existing business processes.	**Ensure that security governance is an antecedent to complete security and process integrity**
79.	It is a continuous process, not just a list of things to complete in order to ensure security governance.	**Control assessment and implementation should be undertaken in a continuous iterative manner** **Control implementation should not be an after-thought**
80.	We have to build around the existing processes. Building up from nothing would be more difficult, it is better to have something to begin with.	**Once needs to understand the organizational context for control implementation.** **Controls cannot be implemented using a "clean slate approach"**
81.	Cleanliness, orderliness	**Security governance controls need to be simple and easy to use**
82.	Continuous improvement	**~~Make sure to have continuous improvement~~**
83.	Standardization	**Establish standardization in the control process**
84.	Systemization	**Create systemization in control development process**
85.	Trust	**Establish trust in the organization**
86.	Timeliness	**Controls should reflect timeliness**
87.	Results-oriented	**Have a result oriented attitude**
88.	Power	**One needs to appreciate the impact of organizational power structures while establishing controls**
89.	respecting the rights of others, including their confidences and personal information	**Respect the rights of others** **Respect other people's confidence** **Respect other people's personal information**
90.	~~Accountability for one's actions.~~	**~~People should have accountability for their action~~**

91.	positive reinforcement for doing the right thing and doing things right;	**Establish positive reinforcement for doing the right thing** **Establish positive reinforcement for doing the things right**
~~92.~~	~~negative consequences for failure to do so~~	~~**Establish clear negative consequences for failure to do the right things**~~
93.	Living in a security conscious culture as reflected in individuals watching out for each other.	**Establish a security conscious culture** **Establish a culture where individuals watch out for each other**
94.	Senior executives "walk the talk," holding themselves visibly accountable to the same policies and procedures that apply to everyone else	**Top management should "walk the talk"** **Top management should be visibly accountable for actions** **Visibility in ensuring the policies and procedures are same for all**
95.	Holding all outside parties (customers, suppliers, vendors, partners, contractors, etc.) to the same standard of care as required of employees, and as appropriate to their roles	**Hold all stakeholders to same standard of care appropriate to their roles**
96.	Using regulation as a catalyst for information security governance	**Use regulations as a catalyst for better security governance practices**
97.	When a culture of security is absent, it turns compliance into a "check the box" exercise instead of substantive, sustained improvement.	**Ensure that compliance is a substantive and sustained improvement in business processes** **Lack of security governance culture turns compliance into check the box exercise**
98.	Security is considered a cost of doing business, not a discretionary or negotiable budget-line item that needs to be regularly defended.	**View security governance as cost of doing business** **Security governance is not a negotiable budget-line item**
99.	Security controls has achievable, measurable objectives that directly align with enterprise objectives.	**Security controls should have achievable objectives** **Security controls should have measurable objectives** **Governance control objectives should align with enterprise objectives**
100	Communication on controls topics is encouraged.	**Encourage communication amongst employees about control issues**
100.	Discussion on controls topics is encouraged.	**Encourage discussion amongst employees about control issues**
101.	Debate on controls topics is encouraged.	**Encourage debate amongst employees about control issues**
102.	An organization should regularly compare and benchmarks its security control state, investments, and actions with others in its market sector and community of practice.	**Compare regularly the security governance state across the industry** **Benchmark security governance practices with industry standards**

		Benchmark security governance investments against industry standards
103.	Security leaders/general auditors/treasurer are well respected in the enterprise culture	**Security leaders should be well respected in the organizational culture**
~~104.~~	~~Security leaders are perceived as valued contributors whose opinions and expertise are sought~~	~~**Perceive security leaders/auditors as valued contributors**~~
105.	General auditors navigate freely across the organization	**Auditors should be able to navigate freely across the organization**
106.	Security leaders regularly collaborate with peers	**Peer collaboration in security governance is important**
107.	Rewards, for security-policy compliance are consistently applied and reinforced.	**Rewards for compliance with policies should be ensured**
108.	Recognition for security-policy compliance are consistently applied and reinforced.	**Apply and reinforce recognition for complying with policies**
~~109.~~	~~Consequences for security-policy non compliance are applied and reinforced.~~	~~**Explain the consequences of non compliance with policies**~~
110.	We grant access to people not positions.	**Grant access to people not positions**
111.	Be aware of morality of your staff. Allow them small things and don't wait for things like notices.	**Be aware of the morality of the staff** **Do not delay small things for bureaucratic reasons**
112.	Keep the ownership of the information.	**Focus on ownership of the information**
113.	Internal satisfaction from what I am doing is very important to me.	**Ensure employee satisfaction**
114.	There has to be proper ways to maintain and integrate the information.	**Maintain and integrate the information properly**
115.	Need to create an environment and a leadership style, culture, values where we encourage internal competition to stay within groups.	**Encourage internal competition to stay within groups** **Create an environment of leadership style and culture to minimize intergroup rivalry**
116.	Systematically structure and level information needs.	**Structure your information needs**
117.	Management should be available when people need assistance.	**Make management/leadership available when the need arises**
118.	Give examples to employees about how something has to be done.	**Training with examples**
119.	Give specific details of what you want and how you want it.	**Provide specific examples of how work should be done**
120.	Information can be improperly integrated. Audit process helps in this.	**Develop audit process to integrate the information rules**

121.	personal integrity influences individual and group behavior towards information security controls	**Personal integrity influences individual behavior towards controls** **Personal integrity influences group behavior towards controls**
122.	Honor: It is important to go beyond disciplinary records to establish whether or not the truth was told even when it would result in a negative outcome for the individual.	**Ensure honor of the employees** **Ensure that truth is being told** **Go beyond the norms to protect honor of individuals**
123.	We all must be able and capable of trusting everyone in the organization that comes into contact with our shared assets.	**Enhance an environment of trust in the organization**
124.	Politics, favoritism, and self-interest typically trump these values and may undermine the security of information systems	**Politics undermines the security governance** **Avoid favoritism in groups** **Avoid self interest in group**
125.	Only individuals with strong moral values are allowed to access, audit, and sustain our information systems.	**Ensure individuals with strong moral values to access data** **Ensure individuals with strong values to audit the systems**
126.	Continuous monitoring is of no use if corrective measures are not instituted and carried out.	**Ensure continuous monitoring of controls** **Institute corrective measures for continuous monitoring**
127.	None of these control measures will work if key individuals and the organization lack the fortitude to enforce the rules and the remedial solutions.	**Ensure that key individuals enforce rules and remedial solutions**
128.	whatever you do.. you should not impede people or hinder people doing their job.	**Do not create barriers to people doing their job**
129.	You should be flexible enough but strong enough to protect companies assets…	**Be flexible and strong to protect company assets**
130.	so you have to put those kinds for things which are acceptable.. and respected by people	**Do things that are acceptable and respected by people**
131.	You have to educate people …why are we doing what we are doing	**Educate people** **Explain to people why they are doing what they are doing**
132.	change management for any kinds of changes….to any production systems ..should go thru proper security channels to make those changes	**Manage changes in the organization properly** **Changes in production systems should be managed**
133.	The ability to share: work, responsibility, and credit, is a fundamental measure of integrity.	**Encourage the ability to share the work** **Ability to share responsibility is important** **Credit about a good work should be shared properly**

		Ability to share is a fundamental measure of integrity
134.	You have to have enough firewalls….routers…software…so that you can protect external threats…	**Have enough technical protections in the organization**
135.	internally people are as bad as they are outside….disgruntled employee can share any access with outside	**Have protection against disgruntled employees**
136.	trust goes so far….there have to be controls…some procedures in place…	**Trust is important in the organization** **Create controls in work process to ensure procedures are followed**
137.	You have to do a risk assessment…for every kind of information..	**Perform a risk assessment to develop controls**
~~138.~~	~~most of the information gets collected from the garbage.. as a part of your security you have to worry about physical security …~~	~~**Physical security is important part of security**~~ ~~**Create controls for accessing information from garbage**~~
139.	You have to worry from both perspective…what's the damage to the organization and what's the damage to the individual…	**Assess the damage to the organization from lack of control** **Assess damage to the individual from lack of controls**
140.	internal control within IT should be such that no person has all the rights	**No single person should have all the rights or access**
141.	If you intend to do something which is different from our standard process you have to be accountable….the manager has to know the process…	**Know the business process properly** **Own up the responsibility for any deviation in the normal business process**
142.	since SOX has come things have changed…companies are spending lot of time in this .	**Regulations have changed the way companies look at controls** **Organizations are spending resources on compliance**
143.	if I were the CIO..I follow through and make sure that we are we have to prove that what we say is what we do	**Ensure what is being claimed is being done**
144.	people do not see any value in those controls…..if you do not see in value some thing …it will not move forward…..	**Ensure that people see value in controls**
145.	all will go lose .. if there is no disciplinary action… if there are no policy published in HR handbook that if you do this thing …. The consequences are such so why would I do that	**Explain clearly the disciplinary actions**
146.	at the beginning if the controls are too complex...people will find a way around it… they do not want to do it…	**Do not make complex controls**
147.	complexity definitely derives adherence ….if they are flexible .. they are good.. people understand ..and they will work… it's not tying	**Explain the purpose of control to people. The complexity derive adherence of controls.**

	my hands.. but helping me to do the work .. I will follow it	
148.	Ease of use…	**Ensure that controls are easy to use**
149.	importance of controls… if I do not see it is important … I will not do it…..why should I do it……	**Communicate importance of controls**
150.	whether it IT function or HR function it has to be function that has to be properly defined…positioned by organization .. funded by the organization.. and respected by the organization where you put ownership of controls does not matter	**Ownership of control should reside in functionality**
151.	Management has to be committed no matter where you put it…	**Management should be committed to controls.**
152.	chances of success of security in being in IT are higher because it is a discipline which brings	**The ownership of control should lies with IT department.**
153.	I think it was a shame not to follow regulations.	**Ensure that the regulations are followed.**
154.	Regulations should be followed in their entirety.	**Follow regulations in entirety**
155.	Certain line of business should be more strict with the following through of such regulations.	**Differentiate between lines of business.**
156.	Prevention Mentality	**Create prevention mentality**
157.	open-mindedness	**Encourage open mindedness to provide inputs.**
158.	biggest influence to individual and group behavior towards IS governance is peer pressure.	**Group behavior is governed by peer pressure.** **Peer pressure influences individual behavior.**
159.	If everyone else is following or not following the policies and also ease of use.	**Ensure ease of use of controls.**
160.	ideally each employee job functions and needs should be looked at and IS designed around that IS needs.	**Ensure job design around IS needs.**
161.	biggest factor for whether a person observes the security policy is if it is convenient or not.	**Create convenient policy**
162.	How much people invest in it if the company makes it their priority so will the people.	**Management should make controls its priority**
163.	Some of these practices work only because they are required through law.	**Ensure regulations are followed**
164.	These laws were created for the good of the company and the investor.	**Regulations protect the organization and the investors**
165.	Discipline	**Encourage discipline in the organization**
166.	Whether one's personal values/norms are the same with the company' or not. If it's not they most like his behaviors would negatively affect the security governance.	**Align personal and organizational values**
167.	if one feels his effort/performance is being reward satisfactory, he would voluntary follow	**Reward good performance**

	the controls.	
168.	If the company has a good environment, where everyone willing to follow the security governance, it will affect one's behaviors towards it.	**Encourage an environment of conformity** **Environment of conformity affects individual behavior**
169.	This risk has been instilled in all of our employees. Each department has IT security liaison that is responsible for the IT security plan is implemented.	**Instill risk consciousness in the employees** **Each department should take care of its controls plan**
170.	I feel the responsibility is very important.	**Encourage a sense of responsibility**
171.	There always needs to be balancing point where the practices that are followed / not followed can be sustained by the losses.	**Balance between gains and losses from the controls**
172.	Practices or governance of one kind will depend on the type of industry it is followed	**Differentiate between type of industry**
173.	there has to be strong leadership, reinforcement a tie between what's being done why and its value and risks and regular user education.	**Provide strong leadership** **Explain the reasons behind organizational actions** **Explain the risks and values of controls to users** **Educate users regularly**
174.	It helps to have IT personnel in visible positions with good commitment from top executives.	**Encourage committed IT personnel to be in visible positions**
175.	individuals should also be honest and determined for security.	**Encourage honesty** **Encourage determination about following controls**
176.	Personal integrity influences information security governance practices	**Encourage personal integrity**
177.	Values of the organization	**Instill good values in the organization**
178.	Culture in the organization	**Create controls culture in the organization**
179.	Attitude of supervisors	**Encourage control conscious attitude of supervisors**
180.	Actions (disciplinary) taken against unethical behavior in general influence individual behavior.	**Take disciplinary action against unethical behavior** **Action against unethical actions influences individual behavior**
181.	Relevance /level of confidentiality of information involved influences behavior.	**Behavior is influenced by level of confidentiality of the information**
182.	Secrecy creates fear, which ultimately leads to someone making a mistake by letting information	**Do not create an environment of fear**

out	
183. A value of mistrust by not developing close relationships with business stakeholders has led to this value of secrecy.	**Discourage secrecy amongst employees** **Discourage an environment of mistrust**
184. Data integrity is critical for many reasons.	**Assess the criticality of data integrity**
185. Confidentiality:	**Ensure confidentiality**
186. How important is the info to the firm?	**Assess the sensitivity of the information**
187. Firm wide policies should be readily available accessible.	**Make the polices readily accessible**
188. Some practices (For SOX, HIPPA) work because the company is faced with strict punishment if they don't do it.	**Create a fear of punishment for organizations** **Establish clear consequences for not complying with laws**
189. Respect for company's rule	**Respect company's rules**
190. Respect for society's laws	**Encourage respect for laws of the society**
191. Dedicated to the company	**Encourage dedication to the company**
192. My pride in myself doing my job to the best of my ability drives me the most.	**Encourage self pride in the job**
193. Relationship with my supervisor and /or those that own the data I manage is important.	**Nurture the relationship with employees**
194. If a person does not come to follow the policies, everyone is exposed.	**Ensure everyone follows the policies**
195. Does it hold to correct people responsible for and failure of protecting this privacy	**Make the correct people accountable for their actions**
196. Does the policy make everyone responsible to protecting the information?	**Make people responsible for protecting the information**
197. free expression	**Encourage free expression**
198. Desire to conform	**Instill the desire to conform**
199. Desire to meet expectations	**Instill the desire into the employees to meet the expectations about controls**
200. Have good changeability	**Encourage flexibility in controls**
201. Communication policy	**Encourage efficient communication policy within the organization**
202. Corporate security control strategy	**Develop corporate security control strategy**
203. Improper business process	**Avoid improper business processes**
204. Risk Management Strategy	**Establish a risk management strategy**
205. This is where the proactive approach of putting	**Establish controls proactively**

	in internal controls (just like burglar bars – against burglars) to ensure that "burglars" are taken care of where there is a breach.	**Ensure that action is taken against people who break the law**
206.	the psychology of the perpetrators should be analyzed from this perspective and strategies put in place for counter measures.	**Analyze the psychology of the perpetrators** **Create counter measures to deal with destructive actions**
207.	The best way to stop this internally is to instill good principals into employees (control from source)	**Instill good principles into employees** **Manage controls from the source of problems i.e. employees**
208.	a big stick for those who break the rules – "whack" them hard so that it be lesson not only for the rule breaker but for anyone who will try to follow suite.	**Establish clear punishments for rule breakers** **Set deterrence criteria to be followed**
209.	IT manages and facilities by installing suitable environmental and physical controls which are regularly reviewed for their proper functioning	**Establish suitable environmental and physical controls** **Regularly review the controls for proper functioning**
210.	**Organizational responsibilities and formal processes for ensuring compliance with external requirements are clearly defined.** **Centralize controls functionality**	**Create organizational responsibilities for compliance** **Formalize process of compliance in the organization** **Develop a central control functionality**

Table: Common Form Values to Objectives

Maximize Internal Controls for IS Security

No.	Common Form Values	Objectives
1.	Lack of awareness is a source of problems.	Increase awareness of security governance
2.	Responsiveness to media hype	Ensure responsiveness media hyped issues
3.	Clarity of responsibility in organizations Accountability for actions	Define responsibility and accountability of controls for security governance
4.	Leverage individual knowledge for ensuring internal controls	Ensure learning about internal control issues
5.	Ensure awareness of organizational actions and practices	Increase awareness of business activities and processes
6.	Training should reflect principles of internal controls rather than means of ensuring security	Define training programs to reflect details of internal controls
7.	Increase awareness of internal control breaches through social engineering	Increase awareness of breaches because of social engineering
8.	Define policies for access to information resources	Define control policies for access to information resources
9.	Define multiple layers of controls	Define multiple layers of controls
10.	Define a system for incorporating feedback to improve controls Balance convenience with usability	Institute feedback channels for security governance Balance convenience with usability
11.	Ensure compliance with internal controls defined in the policy document	Ensure compliance with policy document
12.	Individuals differences in managing internal controls	Manage individual differences about controls
13.	Internal audit control practices need to evolve with time and changing contexts	Develop audit practices for changing contexts of governance
14.	Take input from various individuals dealing with controls on a day to day basis	Incorporate feedbacks from people on daily basis
15.	Auditing and compliance with controls is also based on informal feedback from trusted informants	Encourage informal feedback from people about controls
~~16.~~	~~Sit with people individually and take their perspective on the process~~	
17.	Internal control audit involves cross checking procedures with people	Develop cross checking mechanisms for audit function
18.	Individuals have ability to improve internal controls. Individuals constrained because of resource allocations	Encourage individual to improve controls Discourage individuals from feeling restrained due to resources
19.	Internal control auditors are indeed consultants who ensure effectiveness of controls	Treat internal auditors as consultants to ensure effectiveness of controls

20.	Internal control structures are not static. Proper change management needed for efficacy of controls	Develop dynamic internal control structures Develop effective change management practices
~~21.~~	~~Controls should consider change of roles~~	
~~22.~~	~~Controls need to be tested appropriately~~ ~~Controls are created by the management and employees~~	
~~23.~~	~~High level controls are needed for direction~~ ~~Specific controls use different approaches by organizations~~	
~~24.~~	~~Change management controls are important~~	
25.	Clarity of business processes for internal controls	Establish clarity in business processes
26.	Encourage discussion on internal controls as identified in the policies	Encourage discussion on internal controls as identified in the policies
27.	Be aware of industry frameworks and models. They guide proper internal control formulation.	Refer to industry models and frameworks for control formulation
~~28.~~	~~Generic frameworks need interpretation~~ ~~Following industry frameworks requires preparations~~	
29.	Balancing centralization vs decentralization (move to 9)	Balance centralization with decentralizations
30.	Consequences of internal control breaches should be communicated. (move to under 3 above)	Communicate the consequences of internal controls breaches
31.	Encourage regulatory compliance to internal controls	Encourage regulatory compliance to internal controls
32.	Establish a control consciousness culture Establish a compliance culture	Establish a control consciousness culture Establish a compliance culture
~~33.~~	~~Auditing has gained importance as a functionality~~	
34.	Regulations may be too strong to be followed in entirety – define appropriate internal controls in response to regulations	Define controls for compliance with regulations
~~35.~~	~~Regulations help in following the controls better~~	
36.	Failure to comply with internal control regulations scares people	Explain the consequences of failure to comply with regulations
~~37.~~	~~Repeat compliance with regulations is~~	

	~~difficult~~	
38.	Internal control structures should reflect sensitivity of data	Establish control structure to reflect sensitivity in data
~~39.~~	~~Access to data resources should be restricted~~	
40.	Identify data owners for sensitive data Authorizations should be linked to data owners	Identify data owners for sensitive data Link data owners with authorizations
41.	Encourage individual responsibility for ensuring proper access to data resources.	Encourage individual responsibility for ensuring proper access to data resources.
42.	Top management involvement in defining internal controls for security	Involve top management to defined internal controls
43.	Top management should lead by example when dealing with internal controls	Encourage top management to lead by example
~~44.~~	~~Awareness of compliance issues is important~~	
~~45.~~	~~Direction should be provided from the top management~~	
46.	Role and privileges need to be properly defined and documented ~~Data resources should be clearly classified according to sensitivity level~~	Define and document roles and privileges properly
47.	Communication about the nature and scope of controls is important	Communicate about nature and scope of controls
48.	Education of employees regarding internal controls is needed	Encourage education about internal controls
~~49.~~	~~Executives should be accountable for the actions~~ ~~Rules should be followed~~	
50.	Change attitude of executives about security controls Executives impact the organization's attitude towards security	Change attitude of executives about security controls Not sure
51.	Security requirements define internal controls	Ensure internal controls meet security requirements
52.	Continuously update internal control requirements in security policies	Reflect control requirements in security policies
~~53.~~	~~Education is an important control for security~~	
54.	Controls need to be people oriented. Need to understand feelings, attitudes and belief of people.	Develop people oriented controls Understand people's attitudes and beliefs about controls
~~55.~~	~~Security awareness training is important for good controls~~	
56.	Engage in an IT architecture review, which	Ensure IT architecture review for

	helps in correctness of design All program codes should be adequately reviewed	correctness of design Ensure adequate review of programs
57.	~~Change management process is important~~ All guidelines for governance need to be defined by consensus	~~develop guidelines using consensus~~
~~58.~~	~~Change management should be adequately emphasized~~	
59.	Relevance of all controls needs to be adequately discussed	Discuss adequately the relevance f controls
60.	Controls in business processes are not an after-thought, they are designed and built as part of a change initiative	Develop controls as a part of change initiative
61.	Do not agitate employees	Discourage employee agitation
62.	Sudden changes in responsibility structures are not good for security governance Do not impose new rules on employees without careful consideration and proper buy-in	Discourage sudden changes responsibility structures Discourage imposing ad hoc new rules
63.	~~Demonstrate clearly roles and responsibilities~~ Organizational members need to understand that certain tasks, controls and actions have a priority	~~Explain priotization of tasks and actions for controls to members~~
64.	Auditing functions and actions need to be separated	Establish difference between audit functionality and actions
65.	Controls need to be at all levels of the organization – higher levels as well as lower levels Identity management is perhaps the most important control in organizations	Develop controls for all the levels in the organization Develop identity management control
66.	Controls need to be periodically evaluated by external auditors	Ensure periodic review of controls from external auditors
67.	Controls should be related to the IT architecture Controls need to be instituted as part of organizational design	Establish the relation between controls and IT architecture Institute controls as part of organizational design
68.	There needs to be a management function that ensures efficacy of controls	Ensure efficacy of controls through the management

	~~Separate office is required for maintenance~~	
69.	The nature of controls determines that kind of tools necessary for management Resources need to be allocated for maintaining controls	Develop flexibility in tools for controls Ensure adequate resources allocation for maintenance of controls
70.	~~Accountability and responsibility is required~~ Consequences of non compliance to controls needs to be communicated to the employees	~~Communicate the consequences of non compliance of ontrols~~
71.	Explain the meaning of criminal action to the employees ~~Explain the consequences of action~~	Explain the meaning of criminal action to the employees
72.	Security governance has to be a functional requirement	Develop security governance as a functional requirement
~~73.~~	~~Ensure that companies do the right thing~~ ~~Training is required to help organizations do the right thing~~	
74.	Bridge the gap between different functionalities in the organization MIS and accounting have to coordinate for better controls	Bridge the gap between different functionalities in the organization Encourage co-ordination between MIS and accounting for controls
75.	~~Provide training to technology oriented people such that they are responsive for compliance purposes~~ Explain the importance and need for compliance to technical people	Explain the importance and need for compliance to technical people
76.	~~Better change management practices in the organization~~ Appreciation for cultural aspects needs to be central in organizing security governance controls	~~Encourage appreciation for security governance culture~~
77.	Review of controls should be in light of the organizational objectives	Review controls with respect to organizational objectives
78.	Ensure that security governance is an antecedent to complete security and process integrity	Ensure that security governance is an antecedent to complete security and process integrity
79.	Control assessment and implementation should be undertaken in a continuous iterative manner Control implementation should not be an after-thought	Ensure continuously iterative control assessment and implementation Discourage planning about control implement ion as after thought

80.	One needs to understand the organizational context for control implementation. Controls cannot be implemented using a "clean slate approach"	Understand the organizational context of controls implementation Use clean slate approach for controls implementation
81.	Security governance controls need to be simple and easy to use	Develop simple and easy to use controls
82.	~~Make sure to have continuous improvement~~	
83.	Establish standardization in the control process	Establish standardization in the control process
84.	Create systemization in control development process	Create systemization in control development process
85.	Establish trust in the organization	Establish trust in the organization
86.	Controls should reflect timeliness	Ensure timeliness in controls
87.	Have a result oriented attitude	Develop a result oriented attitude
88.	One needs to appreciate the impact of organizational power structures while establishing controls	Understand organizational power structures in developing controls
89.	Respect the rights of others Respect other people's confidence Respect other people's personal information	Respect the rights of others Respect other people's confidence Respect other people's personal information
90.	~~People should have accountability for their action~~	
91.	Establish positive reinforcement for doing the right thing Establish positive reinforcement for doing the things right	Establish positive reinforcement for doing the right thing Establish positive reinforcement for doing the things right
~~92.~~	~~Establish clear negative consequences for failure to do the right things~~	
93.	Establish a security conscious culture Establish a culture where individuals watch out for each other	Establish a security conscious culture Establish a culture where individuals watch out for each other
94.	Top management should "walk the talk" Top management should be visibly accountable for actions Visibility in ensuring the policies and procedures are same for all	Encourage the management to "walk the talk" Encourage transparency about accountability for actions Enhance visibility about fairness of policies and procedures
95.	Hold all stakeholders to same standard of care appropriate to their roles	Ensure appropriate care to all stakeholders

96.	Use regulations as a catalyst for better security governance practices	Use regulations as a catalyst for better practices
97.	Ensure that compliance is a substantive and sustained improvement in business processes Lack of security governance culture turns compliance into check the box exercise	Ensure that compliance is a substantive and sustained improvement in business processes Avoid turning compliance into check the box exercise
98.	View security governance as cost of doing business Security governance is not a negotiable budget-line item	View security governance as cost of doing business Ensure that security governace is a non-negotiable budget line item
99.	Security controls should be achievable Security controls should have measurable objectives Governance control objectives should align with enterprise objectives	Develop achievable objectives Develop measurable security control objectives Align security control objectives with enterprise objectives
100	Encourage communication amongst employees about control issues	Encourage communication amongst employees about control issues
100.	Encourage discussion amongst employees about control issues	Encourage discussion amongst employees about control issues
101.	Encourage debate amongst employees about control issues	Encourage debate amongst employees about control issues
102.	Compare regularly the security governance state across the industry Benchmark security governance practices with industry standards Benchmark security governance investments against industry standards	Compare the state of controls with standards across industry Benchmark security governance practices with industry standards Benchmark security governance investments against industry standards
103.	Security leaders should be well respected in the organizational culture	Ensure respect for security leaders
~~104.~~	~~Perceive security leaders/auditors as valued contributors~~	
105.	Auditors should be able to navigate freely across the organization	Ensure adequate access to auditors across the organization
106.	Peer collaboration in security governance is important	Encourage collaboration with peers
107.	Rewards for compliance with policies should be ensured	Ensure rewarding for conformity with policies
108.	Apply and reinforce recognition for complying with policies	Provide recognition for complying with policies
~~109.~~	~~Explain the consequences of non compliance with policies~~	
110.	Grant access to people not positions	

111.	Be aware of the morality of the staff Do not delay small things for bureaucratic reasons	Understand the morality of the staff Avoid bureaucratic delays
112.	Focus on ownership of the information	Ensure ownership of information
113.	it is helpful though to have a separate controls department…that would get the money required…	Develop a central controls department
114.	Ensure employee satisfaction	Ensure employee satisfaction
115.	Maintain and integrate the information properly	Maintain and integrate the information properly
116.	Encourage internal competition to stay within groups Create an environment of leadership style and culture to minimize intergroup rivalry	Encourage internal competition to stay within groups Create an environment of leadership style and culture to minimize intergroup rivalry
117.	Structure your information needs	Ensure structuring the information needs
118.	Make management/leadership available when the need arises	Ensure availability of the management
119.	Training with examples	Ensure training with examples
120.	Provide specific examples of how work should be done	Illustrate with specific work related examples
121.	Develop audit process to integrate the information rules	Develop audit process to integrate the information rules
122.	Personal integrity influences individual behavior towards controls Personal integrity influences group behavior towards controls	Encourage personal integrity Respect personal integrity in a group
123.	Ensure honor of the employees Ensure that truth is being told Go beyond the norms to protect honor of individuals	Ensure honor of the employees Ensure that truth is being told Protect honor of the individuals
124.	Enhance an environment of trust in the organization	Enhance an environment of trust in the organization
125.	Politics undermines the security governance Avoid favoritism in groups Avoid self interest in group	Discourage politics in the organization Discourage favoritism in groups Discourage self interest in groups
126.	Ensure individuals with strong moral values to access data Ensure individuals with strong values to audit the systems	Encourage access to individuals with strong moral values Ensure strong moral values in auditors
127.	Ensure continuous monitoring of controls	Ensure continuous monitoring of controls

	Institute corrective measures for continuous monitoring	Institute corrective measures for continuous monitoring
128.	Ensure that key individuals enforce rules and remedial solutions	Ensure that key individuals enforce rules and remedial solutions
129.	Do not create barriers to people doing their job	Discourage impeding people from their job
130.	Be flexible and strong to protect company assets	Protect company assets
131.	Do things that are acceptable and respected by people	Encourage acceptable and respectable actions
132.	Educate people Explain to people why they are doing what they are doing	Educate people Explain the rationale behind controls
133.	Manage changes in the organization properly Changes in production systems should be managed	Manage changes efficiently Manage changes in production systems
134.	Encourage the ability to share the work Ability to share responsibility is important Credit about a good work should be shared properly Ability to share is a fundamental measure of integrity	Encourage the ability to share the work Encourage responsibility charing Encourage sharing the credit for good work
135.	Have enough technical protections in the organization	Ensure adequate technical controls
136.	Have protection against disgruntled employees	Ensure protection against disgruntled employees
137.	Trust is important in the organization Create controls in work process to ensure procedures are followed	Encourage trust Create controls to follow the procedures
138.	Perform a risk assessment to develop controls	Ensure risks assessment to develop controls
~~139.~~	~~Physical security is important part of security~~ ~~Create controls for accessing information from garbage~~	
140.	Assess the damage to the organization from lack of control Assess damage to the individual from lack of controls	Ensure damage assessment to the organization from lack of controls Ensure damage assessment for individuals from lack of controls
141.	No single person should have all the rights	Discourage providing all rights to an

	or access	individual
142.	Own up the responsibility for any deviation in the normal business process	Understand the business processes -
143.	Regulations have changed the way companies look at controls Organizations are spending resources on compliance	Understand the impact of regulations on controls Provide resources for compliance
144.	Ensure what is being claimed is being done	Ensure what is being claimed is being done
145.	Ensure that people see value in controls	Ensure that people see value in controls
146.	Explain clearly the disciplinary actions	Explain clearly the disciplinary actions
147.	Do not make complex controls	Discourage complex controls
148.	Explain the purpose of control to people. The complexity derive adherence of controls.	Explain the purpose of controls
149.	Ensure that controls are easy to use	Ensure that controls are easy to use
150.	Communicate importance of controls	Communicate importance of controls
151.	Ownership of control should reside in functionality	
152.	Management should be committed to controls.	Ensure management commitment to controls
153.	The ownership of control should not lie with IT department	Ensure that IT department does not have the ownership of controls
154.	Ensure that the regulations are followed.	Ensure that the regulations are followed.
155.	Follow regulations in entirety	Follow regulations in entirety
156.	Differentiate between lines of business.	Differentiate between lines of business.
157.	Create prevention mentality	Create prevention mentality
158.	Encourage open mindedness to provide inputs.	Encourage open mindedness to provide inputs.
159.	Group behavior is governed by peer pressure. Peer pressure influences individual behavior.	Understand the group behavior due to peer pressure Understand the influence of peer pressure on individual behavior
160.	Ensure ease of use of controls.	Ensure ease of use of controls.
161.	Ensure job design around IS needs.	Ensure job design around IS needs.
162.	Create convenient policy	Create convenient policy
163.	Management should make controls its priority	Ensure controls are a priority for the management
164.	Ensure regulations are followed	Ensure regulations are followed
165.	Regulations protect the organization and the investors	Ensure regulations protect stakeholders
166.	Encourage discipline in the organization	Encourage discipline in the organization
167.	Align personal and organizational values	Align personal and organizational values
168.	Reward good performance	Reward good performance
169.	Encourage an environment of conformity Environment of conformity affects individual behavior	Encourage an environment of conformity Environment of conformity affects individual behavior

170.	Instill risk consciousness in the employees Each department should take care of its controls plan	Develop risk consciousness in the employees Ensure departments have control plan
171.	Encourage a sense of responsibility	Encourage a sense of responsibility
172.	Balance between gains and losses from the controls	Balance between gains and losses from the controls
173.	Differentiate between type of industry	Differentiate between type of industry
174.	Provide strong leadership Explain the reasons behind organizational actions Explain the risks and values of controls to users Educate users regularly	Provide strong leadership Explain the reasons behind organizational actions Explain the risks and values of controls to users Educate users regularly
175.	Encourage committed IT personnel to be in visible positions	Encourage committed IT personnel to be in visible positions
176.	Encourage honesty Encourage determination about following controls	Encourage honesty Encourage determination about following controls
177.	Encourage personal integrity	Encourage personal integrity
178.	Instill good values in the organization	Ensure good values about security governance
179.	Create controls culture in the organization	Create controls culture in the organization
180.	Encourage control conscious attitude of supervisors	Encourage control conscious attitude of supervisors
181.	Take disciplinary action against unethical behavior Action against unethical actions influences individual behavior	Ensure disciplinary action against unethical behavior Ensure action against unethical behavior
182.	Behavior is influenced by level of confidentiality of the information	Define responsibilities according to level of confidentiality of information
183.	Do not create an environment of fear	Discourage an environment of fear
184.	Discourage secrecy amongst employees Discourage an environment of mistrust	Discourage secrecy amongst employees Discourage an environment of mistrust
185.	Assess the criticality of data integrity	Assess the criticality of data integrity
186.	Ensure confidentiality	Ensure confidentiality
187.	Assess the sensitivity of the information	Assess the sensitivity of the information
188.	Make the polices readily accessible	Ensure policies are readily available
189.	Create a fear of punishment for organizations Establish clear consequences for not	Create a fear of punishment for organizations Establish clear consequences for not

	complying with laws	complying with laws
190.	Respect company's rules	Respect company's rules
191.	Encourage respect for laws of the society	Encourage respect for laws of the society
192.	Encourage dedication to the company	Encourage dedication to the company
193.	Encourage self pride in the job	Encourage self pride in the job
194.	Nurture the relationship with employees	Nurture the relationship with employees
195.	Ensure everyone follows the policies	Ensure everyone follows the policies
196.	Make the correct people accountable for their actions	Ensure accountability
197.	Make people responsible for protecting the information	Ensure responsibility for protecting information
198.	Encourage free expression	Encourage free expression
199.	Instill the desire to conform	Instill the desire to conform
200.	Instill the desire into the employees to meet the expectations about controls	Instill the desire into the employees to meet the expectations about controls
201.	Encourage flexibility in controls	Encourage flexibility in controls
202.	Encourage efficient communication policy within the organization	Encourage efficient communication policy within the organization
203.	Develop corporate security control strategy	Develop corporate security control strategy
204.	Avoid improper business processes	Avoid improper business processes
205.	Establish a risk management strategy	Establish a risk management strategy
206.	Establish controls proactively Ensure that action is taken against people who break the law	Establish controls proactively Ensure that action is taken against people who break the law
207.	Analyze the psychology of the perpetrators Create counter measures to deal with destructive actions	Analyze the psychology of the perpetrators Create counter measures to deal with destructive actions
208.	Instill good principles into employees Manage controls from the source of problems i.e. employees	Instill good principles into employees Manage controls from the source of problems i.e. employees
209.	Establish clear punishments for rule breakers Set deterrence criteria to be followed	Establish clear punishments for rule breakers Set deterrence criteria to be followed
210.	Establish suitable environmental and physical controls Regularly review the controls for proper functioning	Establish suitable environmental and physical controls Regularly review the controls for proper functioning
211.	Create organizational responsibilities for compliance Formalize process of compliance in the organization Centralize your controls functionality. It is important to have all the controls work under the same umbrella.	Create organizational responsibilities for compliance Formalize process of compliance in the organization Centralize controls functionality

Objectives for Maximizing Information Systems Security Governance

1 Fundamental Objectives (condensed after completion of Phase 1)

	Objective Name	Condensed objectives
F1	Ensure corporate controls strategy	Establish security controls as non-negotiable budgetary item Encourage planning about power structures in developing controls Establish security governance as n antecedent to complete security Establish security as cost of doing business Ensure departments have control plan and tools
F2	Encourage a controls conscious culture	Encourage appreciation for prevention mentality Encourage a culture where individuals watch out for each other Ensure an obedient culture
F3	Maximize Clarity in Policies and Procedures	Enhance visibility about fairness of policies and procedures Ensure reflecting control requirements in policies Improve the accessibility of the policies in the organization Encourage discussion on internal controls as identified in the policies
F4	Maximize Regulatory Compliance	Encourage development of controls for regulatory compliance Improve security governance practices using compliance as a 'catalyst' Establish a compliance culture Follow compliance in its entirety
F5	Ensure continuous iterative control assessment	Improve controls implementation practices continuously Encourage validation of controls with changing contexts Establish organizational context for control implementation Enable effective change management practices

Means objectives (Condensed after completion of Phase 1 of the study)

	Objectives	Condensed Sub-Objectives
M1	Ensure Efficacy of Audit Processes	Encourage audit processes to integrate information rules
		Ensure audit practices for changing contexts of governance task
		Ensure adequate access to auditors across the organization
		Encourage internal auditors as consultants to ensure effectiveness of controls
M2	Maximize clarity in business processes	Enable clarity in business related activities
		Ensure sound understanding of business processes
M3	Ensure Communication about Controls	Encourage communicating scope and intent of the controls
		Improve inter and intra group employee communications about controls
		Encourage frequent debates about risks and values of controls
		Explain the damages from lack of controls
		Enable efficient communications policy
M4	Ensure Alignment of Individual and Organizational Values	Encourage aligning personal and organizational values
		Encourage respect for individuals' privacy
		Increase individual loyalty to the organization
		Improve individual's attitudes and beliefs about controls
M5	Ensure data criticality	Ensure data classification according to sensitivity
		Enable data ownership
		Ensure data is linked to authorizations
		Ensure identity management
M6	Ensure punitive structures	Ensure action against unacceptable behavior
		Ensure clear consequences for non conformity
		Encourage defining criminal behavior clearly
		Improve discipline in the organization
M7	Ensure clarity in control development process	Encourage development of simple and easy to use controls
		Ensure timely and flexible controls
		Ensure multi layered nested controls
		Ensure risks assessment to develop controls

M8	Ensure formal controls assessment functionality	Ensure a centralized controls assessment functionality Improve controls as part of organizational design Encourage integration of controls into IT architecture Encourage usability assessment of controls Encourage stakeholder participation in controls Minimize bureaucratic delays Discourage planning about control implementation as "after thought" Ensure balance between gains and losses from the controls
M9	Maximize monitoring and feedback channels	Ensure continuous monitoring of controls Ensure periodic review of controls by external auditors Encourage development of feedback channels for security goervancne Encourage review of controls with respect to organizational objectives
M10	Ensure Visible Executive leadership	Encourage the management to "walk the talk" Encourage top management to lead by example Encourage committed IT personnel to be in visible positions Encourage control conscious attitude of supervisors
M11	Maximize Group Cohesiveness	Encourage sharing the credit for good work Minimize favoritism in groups
M12	Maximize management commitment	Ensure management commitment to controls efficiency Encourage rewarding conformance with controls Increase positive reinforcement for doing the right thing Ensure open environment Discourage impeding people from their job Discourage imposing ad hoc new rules
M13	Maximize resource allocation for controls	Ensure resources for controls Enable appropriate environmental and physical controls Ensure cross functional group agreement on controls
M14	Encourage Standardization of	Encourage benchmarking controls against industry standards

	Controls	Encourage comparison of controls in same line of business
M15	Maximize Training and Education	Maximize regular training with work related examples Improve knowledge about relevance of controls Encourage awareness about control breaches
M16	Ensure ethical and moral values	Encourage individual ethical and moral values Encourage individual self pride in job Encourage morality of the staff
M17	Maximize trust building mechanisms	Increase trust in the organization Reduce fear in the organization Decrease politics in the organization