ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

ASSESSMENT OF INFORMATION SECURITY CULTURE IN THE BANKING INDUSTRY: THE CASE STUDY OF DEVELOPMENT BANK OF ETHIOPIA

BY

GIRUM AYALEW WONDIMAGEGNHU

MBAAF/0199/2006A

Advisor: - Zemenu Aynadis (Asst. Prof.)

JANUARY, 2016

ADDIS ABABA, ETHIOPIA

ASSESSMENT OF INFORMATION SECURITY CULTURE IN THE BANKING INDUSTRY/ THE CASE STUDY OF DEVELOPMENT BANK OF ETHIOPIA

BY

GIRUM AYALEW WONDIMAGEGNHU

MBAAF/0199/2006A

A THESIS SUBMITTED TO ST. MARY'S UNIVERSITY, SCHOOL OF GRADUATE STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTERS OF BUSINESS ADMINISTRATION (ACCOUNTING AND FINANCE)

JANUARY, 2016
ADDIS ABABA, ETHIOPIA

ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

ASSESSMENT OF INFORMATION SECURITY CULTURE IN THE BANKING INDUSTRY/ THE CASE STUDY OF DEVELOPMENT BANK OF ETHIOPIA

BY

GIRUM AYALEW WONDIMAGEGNHU

MBAAF/0199/2006A

APPROVED BY BOARD OF EXAMINERS

___________________________ ___________________________

Dean, Graduate Studies Signature

___________________________ ___________________________

Advisor Signature

___________________________ ___________________________

External Examiner Signature

___________________________ ___________________________

Internal Examiner Signature

DECLARATION

I, the undersigned, declare that this thesis is my original work prepared under the guidance of Mr. Zemenu Aynadis (Asst. Prof.). All sources of materials used for the thesis have been duly acknowledged. I further confirm that the thesis has not been submitted either in part or in full to any other higher learning institution for the purpose of earning any degree.

Name Signature

St. Mary’s University, Addis Ababa

ENDORSEMENT

This thesis has been submitted to St. Mary’s University, School of Graduate Studies for examination with my approval as a university advisor.

Advisor Signature

St. Mary’s University, Addis Ababa

DEDICATION

I dedicate this work to my Wife Tigist Chemir, My beloved son Nahom and my beloved daughter Betselot, My parents Tidenek Tekile and Ayalew Wondimagegnehu for their unconditional love and inspiration.

TABLE OF CONTENTS

Page

Page

CHAPTER THREE RESEARCH METHODOLOGY

CHAPTER FOUR RESULTS & DISCUSSION

CHAPTER FIVE SUMMARY, CONCLUSIONS & RECOMMENDATION

ACKNOWLEDGEMENTS

I am so thankful to the Almighty God who has made it possible, under all circumstances, for me to carry out this research.

I am so grateful to my supervisor Ato Zemenu Aynadis (Asst. Prof.) for his academic guidance, time; encouragement and patience that has seen me through, making this work a success. Special thanks to Development Bank of Ethiopia and employees of the Bank who assisted me while collecting the necessary data for the paper.

I lastly wish to extend my sincere gratitude toward my friends all my group members and all those who have tirelessly guided and encouraged me at all times throughout my course.

Thank you very much and may almighty God reward you abundantly!

LIST OF ABBREVIATIONS AND ACRONYMS

AIRC: Attack Intelligence Research Center

CISF: Comprehensive Information Security Framework

CobiT: Control objectives for information and related Technologies.

DBE: Development Bank of Ethiopia

ICT: Information communication technology

IEC: International Electrotechnical Commission

IOS: International Organization for Standardization

IS: Information System

ISACA: Information System Audit and Control Association

ISCF: Information Security Culture Framework

ISP: Information Security Policy

LIST OF TABLES

LIST OF FIGURE

Page

ABSTRACT

Information security culture is mainly considered as a set of information security characteristics that the organization values. In this paper, an attempt has been made to assess the information security culture of Development Bank of Ethiopia. The study aimed at the assessment of information security in the Bank with an intention of identifying weak links in the existing information security culture of the Bank. To that end, an information security culture assessment model and instrument (A Questioner) were adopted from previous studies. The instrument (customized for the current study) incorporates statements that assess the attitude of employees in the Bank in relation to information security components using a Likert Scale. The study indicated that there is a serious problem of information security culture in the Bank (34.4% of respondents have unfavorable attitude towards information security culture of the Bank in addition to the lack of a formal information security policy in the Bank). The study concluded that the overall information security culture of the Bank is not conducive for the protection of information assets. There is no appropriate foundation for defining how information security should be managed in the Bank and the risk identification process and documentation as well as control mechanisms are unsystematic. The study recommended that the Bank should implement a comprehensive and adequate set of information security components that aid in addressing threats on the technical, process and people levels based on identified information security risks and the appropriate controls that are necessary to mitigate identified risks. The Bank should adapt and implement International standards such as the Information Security Forum (ISF 2008), the Control Objectives for Information Technology (CobiT 2004), the Information Systems Audit and Control Association (ISACA 2008) and ISO/IEC 17799 (2005) to implement and manage information security components.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy. The Banking industry is among the leading industries in our country that is becoming heavily dependent on ICT for its service provision and other purposes. Banking business competition has stirred the advancement of services enabled by IT which in turn increased the information security risk (Abiy and Lemma. 2012)

Organizations' heavy reliance on information systems (IS) requires them to manage the risks associated with those systems. Today, risks related to information security are a major challenge for many organizations, since these risks may have dire consequences, including corporate liability, loss of credibility, and monetary damage (Cavusoglu, 2004). Ensuring information security has become one of the top managerial priorities in many organizations (Brancheau *et al.* 1996).

Generally speaking information security is the result of the interaction of three things technology, process and humans. Humans are consistently referred to as the weakest link in security (Schneier, 2000). Evidence suggests that, regardless of the number of technical controls in place, organizations will still experience security breaches (Schultz, 2005). Some evidence suggests that employees' failure to comply with information security guidelines is the cause of the majority of breaches in information security (Chan, 2005). A homeowner could implement burglar proofing at each window, but upon leaving the house leave the front door unlocked. The security measures are therefore ineffective due to his behavior. In the same way, organizations implement security controls such as anti-virus programs, firewalls, and passwords. There is no sense in implementing these controls if users share passwords and connect through dialup to the Internet, by passing the firewall (Da Veiga, 2008).

The manner in which employees perceive and interact (behave) with controls implemented to protect information assets is one of the main threats to the protection of such assets and the effective use of information security controls. Despite adequate technical and procedural controls in place if the interaction between employees and information assets is not conducive to the protection of information assets, it has a profound impact like loss of working hour, disclosure of information to unauthorized people, and non compliance of legal and regulatory requirements (Da Veiga, 2008).

To reduce these risks and ensure information security, organizations often rely on technology-based solutions (Ernst & Young 2008). Although these types of solutions help improve information security (Straub 1990), relying on them exclusively (or excessively) is seldom enough to eliminate the risk (Cavusoglu *et al*. 2009). Empirical and anecdotal evidence indicates that the number of incidents related to information security is increasing even as organizations invest more in technology-based solutions.

Studies have also shown that non-technical issues are as important as technical issues in safeguarding an organization's sensitive information (Dhillon, 2006).Technical security controls are necessary but they have to be correctly specified, designed, developed, implemented, configured, used and maintained - steps which all involve human beings. An exclusive focus on the technical aspects of security, without due consideration of how the human interacts with the system, is clearly inadequate. Success in information security can be achieved when organizations invest in both technical and socio-organizational resources (AIRC, 2008).

An information security culture is defined as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e. incidents) evident in artifacts and creations that become part of the way things are done in an organization to protect its information assets. This information security culture changes over time (Da Veiga, 2008).

An information security culture concerns the manner in which employees perceive and interact (behave) with the controls that are implemented to protect computer and information systems and assets in the organization.

The Information Security Forum (ISF 2000) argues that it stems from the interaction of employees with the organization's systems and procedures to influence their behavior ('the way we do things around here'). Employee behavior stems from the values and attitudes adopted by employees, as well as from what is required by the organization's systems and procedures. The behavior exhibited can result either in the protection of information assets or in incidents compromising the protection of information.

According to Schlienger and Teufel (2005) an information security culture is ultimately visible in the beliefs, values and artifacts of an organization. For instance, the employees could believe that they are responsible for the protection of information. As a value the organization could focus on innovation and state-of-the-art technology. Information security induction training could be visible as an artifact.

According to McIlwrath (2006) two to three percent of an organisation's annual profit is potentially lost due to information security incidents. Employees are involved in up to 80% of information security incidents (Walton CB & Walton- Mackenzie Limited 2006). It is clear from these statistics that organizations are potentially losing profit as a result of incidents caused by employees. This view is further supported by a survey conducted by Price Waterhouse Coopers (PWC 2004) which concluded that "human error rather than technology is the root cause of most security breaches". As such the human element, which poses the greatest information security threat to any organization, urgently needs to be addressed (Furnell, 2004).

The effectiveness of internal controls designed to protect the integrity, availability and reliability of information and information technology (IT) systems depends on the competency and dependability of the people who are implementing and using them (Kruger & Kearney 2006). The board of directors, having ultimate responsibility for oversight of the financial reporting process (Deloitte & Touche et al. 2004), must ensure that effective controls are implemented to minimize this risk.

One measure that could be considered to reduce the risks posed by inside employees is to focus on a security-aware culture (Furnell, 2007). To manage their security risks, organizations must have a strong culture of security awareness (information security culture) (Von Solms 2006). This will aid the board of directors to govern the protection of information and to minimize human error or circumvention of controls. Tessem and Skaraas (2005) sustain the notion that an information security culture is vital and must be implemented (cultivated) as part of the general organizational culture. This would not only minimize the threat posed by employees, but also improve the security level and success of the whole organization (Vroom & Von Solms, 2004).

1.2 Statement of the Problem

The banking industry in Ethiopia is among the fastest growing sector in the economy and it is the sector that is fast embracing information technology for its service delivery and financial reporting. The banking industry is also heavily investing on IT services and related infrastructure and becoming heavily dependent on the safe operation of the Information system. DBE is among the Banks that has implemented core banking technology for its main service. As the reliance and dependence increases on IT the associated security risk to the information system and other related assets of the organization will rise.

The main problems observed in the Bank include incorrect loan data capturing, e.g. the system shows abnormal balance after a borrower settled its debt and not capturing the required data at the right time; Non compliance with the Bank's Procedure manual; in ability to detect and rectify problems at early stage; weak internal help desk; Heavy Reliance on few personnel to undertake complicated operations on the system; and manual intervention and system disruption; such problems severely damage the integrity of the data and results in both financial loss and loss of customers' and stakeholders' trust.

Source: Internal Reports of the Bank (2015)

1.3 Research Questions

The major research questions are as follow:

1. Are there adequate leadership and governance that manages the overall information assets at Development Bank of Ethiopia?
2. Are there adequate information security activities such as devising policy, standards, and procedures that govern the overall information technology related activities at Development Bank of Ethiopia?
3. Is there adequate awareness among employees about information system security in Development Bank of Ethiopia?
4. Is there adequate technological protection by the system employed by Development Bank of Ethiopia?
5. Is there a dedicated information security department that controls the overall information security at Development Bank of Ethiopia?

1.4 Objectives of the Study

The general objective of this research is to assess the role of Information security culture at development bank of Ethiopia towards the protection of information assets of the bank in general.

Specifically, this study intends to achieve the following objectives:

1. To assess employees' attitude about the information security leadership and governance in the Bank.
2. To examine employees' attitude about the information security Policies, Procedures, Standards, and Guide lines in the Bank.
3. To examine employees' attitude about information security management and organization related to information security in the Bank.
4. To assess employees' attitude about information security monitoring and compliance and audit in the Bank.
5. To assess employees' attitude about security management related to user (employees) in the Bank.
6. To assess employees' attitude about technical and physical mechanisms implemented to secure an IT environment in the Bank.
7. To assess employees' attitude about change aspects regarding information security in the Bank.

1.5 Definition of Terms

In order to avoid any misunderstanding, it is important to correctly interpret the terminology used in this thesis.

Organizational or Employee behavior

Employee or organizational behavior is an interdisciplinary field dedicated to the better understanding and management of people at work (Robbins, 2001). There are three basic levels of behavior in an organization, namely the individual, group and organizational level (Robbins. 2001). Employees will behave according to what is perceived as correct and acceptable and specific organizational behavior will surface on each level. Such behavior also encompasses employee attitudes and the way in which they influence actual performance in organizations.

Organizational culture

Schein (1985) defines culture as “a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration – that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems”.

Information Security Culture

An information security culture is defined as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization’s systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e. incidents) evident in artifacts and creations that become part of the way things are done in an organization to protect its information assets. This information security culture changes over time(Da Veiga,2008).

Organizational Information Assets

The ISO 17799 (2005) defines an asset as anything that adds value to the organization. This would include information, for example contracts, training material and strategies; software such as system software and utilities; physical assets such as computer equipment; services like communication services and other utilities such as power and lighting; people with their skills and experiences, and lastly, intangible assets such as the image and reputation of the organization.

Every organization uses information as it is an important asset to the business (IS0 17799, 2005). Information is present in many forms, for example in paper and electronic documents; voice recordings and conversations. It is stored in electronic databases, backups, archives and hard copy files; transmitted electronically or by post and even as films and SMSs.

Confidentiality

Confidentiality concerns the protection of sensitive information from unauthorized disclosure. Consideration needs to be given to the level of sensitivity to the data, as this will determine how stringent controls over its access should be. Management need assurance of the organization’s ability to maintain information confidential, as compromises in confidentiality could lead to significant public reputation harm, particularly where the information relates to sensitive client data.

Integrity

Integrity refers to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations. This is an important audit objective to gain assurance on because it provides assurance to both management and external report users that the information produced by the organization's information systems can be relied and trusted upon to make business decisions.

Availability

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities. Given the high-risk nature of keeping important information stored on computer systems, it is important that organizations gain assurance that the information they need for decision-making is available when required. This implies ensuring that the organization has measures in place to ensure business continuity and ensuring that recovery can be made in a timely manner from disasters so that information is available to users as and when required.

1.6 Significance of the Study

The findings of this study have revealed the status of information system security culture of Development bank of Ethiopia. In addition the findings will helped to understand and explain determinants of information system security culture in the Bank. Moreover recommendations given based on the research findings will help the Bank to nurture positive culture that supports information security in the Bank. Banks in Ethiopia with similar firm characteristics can benefit from findings and recommendations of this study.

1.7 Scope of the Study

Information security research is conducted in a variety of academic disciplines such as Computer Science, Informatics, Economics, Industrial Psychology, Information Systems, Management Information Systems, Mathematics and Statistics (De Veiga, 2008). This thesis relates to a specific research category that spans Information technology discipline and Industrial psychology academic disciplines in order to achieve the research objectives. The research category of this study is related to information security and more specifically information security culture. The subject field is narrowed down to information security culture by focusing on the human element (personnel) and employee's interaction with information assets, which further relates to human sciences and culminates in industrial psychology. Hence the study excludes technical (technological) factors that affect information security system at the Bank. This may hinder the researcher from knowing the complete package of the problem at hand. The study focuses on employees at the head quarter of Development Bank of Ethiopia located in Addis Ababa.

1.8 Limitations of the Study

Although this research is prepared very carefully, there is unavoidable limitation as participants in the study may not represent the whole bank as employees at the twelve networked Branches of the bank and other employees who do not have direct contact with the core banking system are excluded from the study.

1.9 Organization of the Study

The research is organized into five chapters. The first chapter deals with introduction part of the study providing details associated with the background of the study, statement of the problem, research questions of the study ,objectives of the study, definitions of key terms, significance of the study, scope of the study, and limitations of the study. In Chapter 2 extensive literature review is presented, chapter 3 deals with the methodology of the study, chapter 4 is dedicated to data presentation, results analysis and discussions. The last chapter 5 is composed of Summary of the main findings, conclusions and recommendation. In addition to the above main contents, list of reference materials and Annex are added at the end of the paper.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

2.1. What is Information security?

Information security refers to the protection of the confidentiality, integrity, and availability of computerized data and of the systems that process, maintain and report these data; during processing, storage and dissemination of output (Kruger, 2006). As with other business assets, information requires protection to ensure that it is available and confidential and that its integrity is preserved where necessary (Pfleeger,1997).

Information security provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted; ensure IT services are usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it (CobiT, 2004).

Threats such as data theft, fraud, fire, viruses, denial-of service attacks and even social engineering pose serious risks to the protection of information (Pfleege,1997). These threats, together with careless mistakes and employee ignorance in respect of security controls could lead to severe financial, reputational and other damages to an organization.

Information security is about implementing adequate controls to protect information assets. Controls must be aligned with the organization’s security objectives and should minimize the risks to which the organization is exposed (ISO 17799, 2005). Controls cover a wide spectrum of technology such as firewalls, processes such as change management, and human elements such as information security induction training.

2.2. What is Information Security Culture?

Martins & Eloff (2006) broadly defined Information security culture as a set of information security characteristics that the organization values; the assumption about what is acceptable and what is not in relation to information security; the assumption about what information security behavior is encouraged and what is not; and the way people behave towards information security in the organization.

An information security culture develops as a result of users’ interaction with information security controls such as passwords, access cards or the use of anti-virus software (Grant 2005). One way of positively directing the cultivation of an information security culture in an organization is to implement information security awareness programs (Drevin, 2006). Another is to use a set of principles designed to cultivate an information security culture that is conducive to the protection of information assets.

Security-aware managers, staff and information technology professionals make better use of technical security controls (Rotvold, 2008). Protecting information used in the wider context should therefore also incorporate the behavior of people. People manage the information in an organization and interact with information technology systems. In line with this (Williams, 2009) noted that the human component is a significant factor in information security, with a large number of breaches occurring due to user error. Technical solutions can only protect information so far and thus the human aspect of security has become a major focus for discussion. Therefore, it is important for organizations to create a security conscious culture. Hence, a positive information security culture can aid in minimizing the people threat compromising information security while interacting with information technology systems (Eloff, 2000).

Martins (2006) also make clear that a certain level of information security culture is already present in every organization using IT, but this culture could be a threat if it is not on an acceptable level. The aim in assessing that culture is to advance it to an adequate level. This could then aid in minimizing internal and external threats to information in the organization. They further stated that people are the center of every activity. Protecting information used in the wider context should therefore also incorporate the behavior of people. People manage the information in an organization and interact with IT systems.

Each organization has its own information security culture similar to every person having their own personality. A positive information security culture can aid in minimizing the people threat compromising information security while interacting with IT systems. The behavior of employees towards information must be acceptable and needs to be part of everyday life in the organization. Every organization also has certain information security practices, which are followed and incorporated into the working environment. To facilitate the above, it is necessary to cultivate an information security culture in the organization (Eloff, 2000).

Through the culture it will be clear what behavior is accepted and encouraged and what is not. To establish the desired culture in an organization, it is necessary to take a look at the organizational behavior of the employees. The type of culture in an organization can have a direct impact on the behavior and actions of the organization’s employees (Martins, 2006). In an organization with a bureaucratic culture, where everyone has to play by the rules, employees might follow the information security policy more strictly than in a less formal and individualistic culture.

When considering the cultivation of an information security culture, the focus is on how to develop such a culture up to an acceptable level in the organization and so protect its information assets. Determining whether the information security culture is on an adequate level requires that a value for it be determined. An acceptable level of information security culture is defined as the level that provides adequate protection to information assets and so succeeds in minimizing the threat to the confidentiality, integrity and availability of the information asset (Da Veiga, 2008).

Assessing human behavior and specifically information security behavior is a mystery to many who are responsible for information security (Vroom, 2004). Metrics are available to assess changes in information security awareness, such as the number of reported security incidents or percentage of paper waste being shredded (Tesseman, 2005). However, assessing an information security culture is more difficult, as security is part of the organization's business processes (Tesseman, 2005).

It is, however, important to assess information security culture in order to identify whether the culture is conducive to the protection of information assets. Should it not be, the assessment results can be used to identify remediation action plans to positively influence the information security culture.

2.2.1. Information security culture and Organizational culture

Probably the best-known definition of Organizational culture is "the way things are done here" (Lundy, 1996). Organizational culture can be seen as the personality of the Organization (Robbins, 2001).

An organizational culture develops on the basis of certain activities in the Organization, such as the vision of management and the behavior that employees exhibit on an individual, group and Organizational level (tier) (Hellriegel, 1998). The organizational culture that develops on the basis of the exhibited behavior is evident in artifacts (locked door), values ('employees are valuable assets') and basic assumptions ('the Information Technology department is responsible for the security of information assets (Schein, 1985). According to Robbins (2001), Organizational behavior is about what people do in an Organization and how their behavior affects the performance of the Organization. The term also incorporates employee attitude and how it relates to the behavior of employees in the Organization (Hellriegel, 1998).

An information security culture develops due to the information security behavior of employees in the same manner that an Organizational culture develops due to the Organizational behavior of employees in the organization (Martins 2002). An information security culture is therefore based on the interaction of employees with information assets and the security behavior they exhibit.

2.2.2. The interaction between information security, behavior and culture

The interaction between information security components (e.g. a policy and the behavior of employees) has an impact on the information security culture that emerges.

Information security components are implemented in the Organization. These components can be seen as the input that *influences* information security behavior in the organization. Implementing the information security components impacts on the interaction of employees with information assets, and employees consequently exhibit certain behavior referred to as information security behavior (Martins, 2002).

The objective is to instill information security behavior that is conducive to the protection of information assets based on the organization's information security policies and code of ethics. Such behavior could involve the reporting of security incidents, adherence to a clear desk policy or the secure disposal of confidential documents. In time, this security behavior evolves as the way that things are done in the organization and an information security culture is therefore established (cultivated). A culture is thus promoted in which ensuring the security of information is accepted as the way things are done (Martins, 2002).

To illustrate the interaction the following example is used. The information security policy, one of the information security components, is used to provide employees with a clear understanding of management's direction and support for information security (ISO/IEC 27001 2005). According to Whitman (2003), the objective of a policy is to influence the decisions, actions and behaviors of employees. It further specifies what behavior is regarded as acceptable and what not. For instance, the information security policy may state that a laptop must be physically secured at all times. The statement in the policy is aimed at directing employee behavior to protect both the physical asset and the data saved on the laptop. The objective is to influence the employee's behavior when interacting with the laptop to ensure the protection thereof. Without this statement and its enforcement, employees could leave their laptops unsecured. Therefore, without information security components to direct and influence employee behavior, employees could well interact with information assets in ways that would introduce risk. In time, such potentially harmful behavior could unfortunately give rise to a culture where neglect is regarded as acceptable. (De Veiga, 2008)

To administer a positively acceptable level of information security, organizations should ensure that a comprehensive and adequate set of information security components is implemented. This set of information security components aids in addressing threats on the technical, process and people levels, in other words threats that would negatively influence the establishment of an acceptable information security culture within the organization. Organizations should furthermore ensure that employee interaction is in line with the requirements of the information security policy. These requirements could involve actions such as making back-ups to the server on a daily basis, password protect information on removable media or the deletion of unsolicited e-mails with attachments.

The components are implemented by the organization on the individual, group or organizational tier of information security behavior. As such, information security behavior is influenced and exhibited on each behavioral tier.

The *individual* tier relates to individuals in the organization who display characteristics that may influence their behavior at work (Robbins, 2001). These characteristics could involve biographical features such as age or marital status; personality characteristics; inherent emotional frameworks; values; and attitudes and basic assumptions (Robbins, 2001). They could affect the behavior of individuals regarding compliance with information security policies. For example, if one considers two types of personalities (A and B), there could be a distinct difference in the way they comply with the information security policy (Robbins 1998: 65). Type A employees emphasize quantity over quality. They work fast and illustrate their competitiveness by working long hours, but often make poor decisions because they make them too fast. Type B employees focus on quality and never suffer from a sense of time urgency. Type A employees, again, might be too hasty to select a strong password. They might share passwords to easily access information rather than to wait for the authorized user to return to access a system. Type B might think twice before making a decision and would probably take a few seconds more to decide on a stronger password. Information security components that positively influence the individual’s information security behavior should therefore be implemented on the individual tier.

The *group* tier focuses on the behavior of people in groups and on the ways in which these groups function (Robbins, 2003). It is important for management to consider employees as members of a group (e.g. a department, team or committee) (Robbins, 2001) and to use the group to establish an acceptable level of information security culture. The group's view or pressure could override the individual's moral judgment and mental efficiency/deficiency – referred to as groupthink (Robbins, 2001). Strong leadership is required to guide groups in making the right decision and to comply with company policies (e.g. not to copy and distribute pirated software).

On the *organizational* tier, formal structures are added. These regulate whether the organization operates in a centralized or decentralized manner. Other considerations involve for instance whether a wireless network should be introduced for constant access to e-mail and what security measures should be implemented to protect information. The formal structures implemented by the organization influence employee attitudes and have an impact on their behavior (Robbins, 2001).

Information security behavior that is sustained over time evolves into an information security culture that is evident in artifacts, as well as in the values and assumptions of employees. Artifacts like technology are usually visible in the organization, for instance public key encryption. Values reflect the sense of what ought to be, or the beliefs of the individual ("I ought to have privacy when using electronic communication"), while basic assumptions are related to the subconscious and are part of human nature ("My manager's decision counts above mine") (Schein, 1985).

The information security culture that is cultivated influences the effectiveness of the information security components. If employees find the information security policy contents difficult to understand or if they consider it not applicable to their business unit, they might refuse to comply with the requirements of the policy. The information security component (policy) implemented is therefore ineffective and employees could introduce intentional or unintentional threats to the environment. This policy must consequently be adjusted and the effect of the change on the organizational level be managed appropriately.

To illustrate the interaction the following example can be considered. A formal information security sponsor may be appointed on the organizational tier. This appointment may influence employees to realize that it is important to invest time and money in information security. It could promote the value of responsibility from a senior level. Finally the information security culture could manifest itself on the artifact level – for example, the information security sponsor would be an executive employee who is included in board committee meetings.

2.3. A Framework for Information Security

Organizations need a systematic information security approach that is used for the arrangement or structuring of information security components to implement information security in an effective manner to mitigate risks in an organization. (De Veiga, 2008)

An information security component is considered as a part of an information security approach that contributes to the implementation and maintenance of information security. In other words, determining what must be implemented or considered by the organization in terms of information security – such as an information security policy, risk assessments, technical controls and information security awareness.

Various researchers propose different approaches towards information security that an organization can use to assist management in implementing information security components. They structure information security components in what can be referred to as an information security framework, model or standard.

This framework, model or standard can be utilized to direct employee behavior in all required facets of information security and cultivate an acceptable level of information security culture. The components can also be used to set key behavior traits. Ultimately they will serve as a guide in developing an information security culture assessment tool with which to assess whether the level of information security culture contributes to or negatively impacts on the protection of information assets.

When considering the cultivation of an information security culture, the focus is on how to develop such a culture up to an acceptable level in the organization and so protect its information assets. An organization that aims to cultivate an acceptable level of an information security culture would require a single, all-encompassing (considering all the relevant focus areas from the current research approaches) approach that can be used in organizations from any environment or of any size.

Again (De Veiga, 2008) has developed a Comprehensive Information Security Framework (CISF) that incorporates the information security components identified through the investigation of existing information security components.

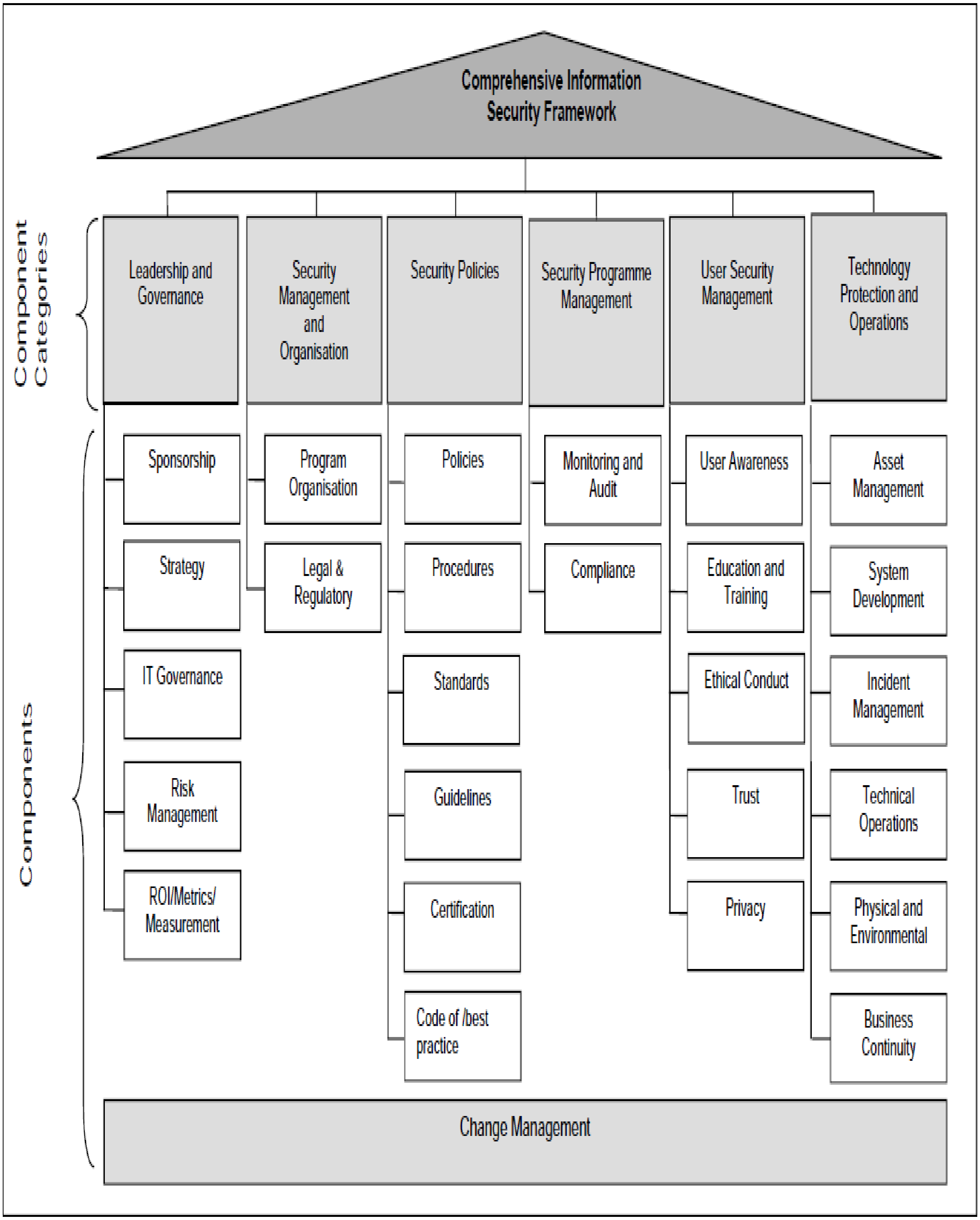

Figure 2.1. Comprehensive Information Security Framework (CISF)

The components of CISF are structured in six component categories comprising of the components listed in figure 2.1. The components are depicted in the categories to illustrate similar concepts that are addressed by the various components. Furthermore components that are of a strategic and managerial nature are depicted on the left side of the framework illustrated in Figure 2.1, thus providing direction to the technical implementation and protection of assets on the right side of the framework. Change management is depicted at the bottom of the framework so as to illustrate that it should be considered across all the component categories.

2.4. Components of information security

Adele has developed comprehensive list of information security components that could influence information security culture in an organization. The different components are defined below.

2.4.1. Leadership and Governance Component

These components are of a strategic nature and provide direction for the implementation of the components in the other categories. It includes sponsorship, strategy, IT governance, Risk management, and ROI /metric /measurement.

Sponsorship: This component refers to an executive sponsor that supports the information security strategy and provides guidance with regard to information security in the organization (Schiesser, 2002). An executive sponsor will typically sit in on the executive board meetings and present information security as an item of the agenda.

Strategy: An information security strategy involves the creation of a strategic vision and plan to address information security risks, but also to meet business objectives (Sherwood, 2005). The information security strategy should be linked to the organizational and IT strategy to ensure that the organization’s objectives are met both in the short and the long term.

IT governance: IT governance is concerned about the policies and procedures that define how an organization will direct and control the use of its technology and protect its information (Posthumus, 2005).

Corporate governance can be explained as the direction and management of a set of policies and internal controls in an organization. Information security governance relates to the commitment of the organization’s executive board to information security and the management of information security through policies, procedures, processes, technology, compliance enforcement mechanisms, as well as awareness initiatives for users (Von, 2006).

Risk management: Risk management is a process for resolving risk. The process includes risk assessment to define the risk, and risk control to resolve the risk (Hall, 1998). Information security risks such as the threat of viruses, hackers or natural disasters need to be identified and the control implemented by considering a cost benefit analysis.

ROI /metric /measurement: Return on investment in terms of information security refers to spending resources. These resources could be money, time and effort so as to gain something – for instance, more secure systems or fewer information security incidents. In order to illustrate a return on investment, the information security efforts have to be measured using metrics (Sherwood, 2005); for instance measure the number of incidents, the time taken to resolve incidents or the number of users who attended the information security induction presentation.

Without sponsorship, IT Governance, and strategy, the appropriate direction for the remainder of the components cannot be provided. Risk management being part of this category serves as the input for defining the level of protection required and provides direction in terms of strategy. For instance, the risk of threats to information in a bank is much higher as opposed to a retail store. Hence the information security strategy of these organizations will be different based on the risk profile of each. Metrics and measurement also provide input to the direction as they aid the organization in assessing the overall success of the information security function and to identify remedial actions (De Veiga, 2008)

2.4.2. Security Management and Organization Component

This category comprises of components that aid in managing information security in the organization and advise how to structure the information security office by also considering regulatory requirements. The components grouped in this category relate specifically to the processes and structures of the information security function.

Program organization: Program organization refers to the information security organizational design, composition and reporting structures (e.g. centralized or decentralized management of security). It also incorporates the roles and responsibilities, skills and experience, and resource levels committed to the enterprise’s security architecture (McCarthy & Campbell 2001). Information security responsibilities within the organization should be allocated in terms of its information security policy. An example of an information security role is the Information Security Officer who is responsible for the management of information security or the network specialist who will ensure that the network is configured in a secure manner. Organizing and formally defining the information security roles will aid in providing a clear definition of the department's hierarchy and authorities.

Legal and regulatory components involve compliance with legislation: Different pieces of national and international legislation need to be considered for information security.

2.4.3. Security Policy Component

This category consists of the documented requirements defined by the organization and international standards or guidelines to direct employee behavior.

Security policies, procedures, standards and guidelines: ISO/IEC 17799 defines a policy as the "overall intention and direction as formally expressed by management". In other words, it is a document detailing what management expects of employees in terms of protecting information assets and is usually not technology specific. An example is an Information Security Policy stating that access should be controlled. A procedure provides the detailed steps of a component mentioned in a policy, for instance the process of granting access and distributing passwords. A standard details the minimum requirements, for instance that a password must be at least 8 characters long and consist of alpha-numeric characters. A guideline is a document that assists management in the implementation of information security.

Certification: Organizations can certify against international standards such as ISO/IEC 17799 (2005). The Financial Services Authority (FSA) recommends certification against ISO/IEC 17799 (2005) as it aids in meeting many regulatory requirements relating to information security.

Best practice or code of practice: International standards such as the Standard of Good Practice from the Information Security Forum (ISF 2008), the Control Objectives for Information Technology (COBIT) from the Information Systems Audit and Control Association (ISACA) (COBIT 2004, ISACA 2008) and ISO/IEC 17799 (2005) are examples of best practices that can be used by Organizations to implement and manage information security.

2.4.4. Security Program Management Component

This category refers to the components that are deployed to ensure the effective management of information security. Monitoring and compliance as well as auditing are included in this component category to manage the security program.

Monitor and audit: Organizations need to monitor their compliance with regulations as these could change over time. Furthermore, since users may not always comply with the requirements, they need to be monitored. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organization (Von, 2006).

Compliance: Compliance relates to ensuring that the organization complies with international and national laws as well as industry regulations pertaining to the protection of information (Sherwood, 2005). It is essential to measure and enforce compliance, and both technology and employee behavior should be monitored to ensure compliance to information security policies and to respond effectively and timely to incidents that are detected (Von, 2006).

2.4.5. User Security Management Component

This category involves those components that relate to the employees in the organization and ways of directing their behavior. As such, processes like education and training, as well as concepts like trust are depicted in this category as they relate specifically to the people component of information security.

User awareness: McIlwraith (2006) believes that awareness is the "single most effective thing an information security practitioner can do to make a positive difference to their organization". Awareness can be explained as the different activities that the organization deploys to reinforce information security requirements and responsibilities required by the information security policy.

Education and training: ISO/IEC 17799 (2005) states that "all employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies, procedures, as relevant for their job function". Users must therefore receive training, which could include induction training presentations, Web-based training or group discussions.

Ethical conduct: Hellriegel, Slocum and Woodman (1998) define ethics as the values and rules that distinguish right from wrong. For example, employees should not talk about confidential information in public places.

Trust: Trust is important when implementing information security. It aids in providing confidence to information users when making decisions. Martins (2002) defines trust as "the process in which a principal relies on a trustee (a person or group of people) to act according to specific expectations that are important to the principal without taking advantage of the principal's vulnerability". When implementing the information security components, management must be able to trust employees to adhere to information security policies, while employees must be able to trust management to illustrate commitment to information security (trust is seen as the primary attribute of leadership) (Robbins, 2001). A trusting relationship should also be established between trading partners and clients who could contribute to the Organization's reputation. One possible way of establishing such a relationship could be for the organization to illustrate that information and assets are secured and that employees comply with requirements.

Privacy: Privacy is an essential issue of trust. Without privacy there is no trust (Borking, 2006). When implementing information security privacy, both employees and customers must be considered and controls must be implemented to protect the personal identifiable information of an individual (ISACA, 2008). An identification number, name and surname or address are examples of personal identifiable information. The organization has to ensure that adequate controls are in place to protect personal information of employees, contractors, customers and third parties.

2.4.6. Technology Protection and operations Component

These components involve the technical and physical mechanisms implemented to secure an IT environment. All components relating to the technology component of information security are grouped together. When implementing the information security framework, the technology controls applicable to the organization's environment and identified risks must be implemented. These include asset management, system development and/or acquisition requirements, incident management, technical operations such as network security, and physical, environment and business continuity controls.

Asset management: Asset management relates to the protection of organizational assets, which includes the identification of assets and maintaining an inventory thereof. It also incorporates the protection of information by classifying it based on the degree of sensitivity and criticality (ISO/IEC 17799:2005).

System development: This component addresses security in system files and the development of new application system software. It also ensures that the change control process followed considers security (ISO/IEC 17799:2005).

Incident management: Incident management is the process used to identify, respond to and monitor information security incidents (ISO/IEC 17799:2005). An information security incident could be a virus affecting the organization's network, a stolen laptop or sharing of a password between employees.

Technical operations: Technical operations refer to the technology used to protect the environment and information assets for instance anti-virus software, firewalls and network configuration, capacity and configuration management (ISO/IEC 17799:2005).

Physical and environmental components: Physical and environment components relate to the protection of the security perimeter and secure areas such as a server room by, for instance, access cards. It also includes protection against environmental threats such as fire, for which a fire extinguisher is needed (ISO/IEC 17799:2005).

Business continuity planning (BCP): Business continuity involves the prevention and mitigation of disruption, as well as the recovery of the business (processes, people and technology) from a disruption (ISACA 2008). A disruption could be a power failure or an earthquake affecting the LAN connectivity between offices. Disaster recovery is part of business continuity. Schiesser (2002) defines disaster recovery as "a methodology to ensure the continuous operation of critical business systems in the event of widespread or localized disasters to an infrastructure environment". An organization has to identify its critical business systems and ensure that there is a plan in place to recover these systems. The plan could for instance involve another site where the environment is duplicated, and the making and off-site storage of such backups.

2.4.7. Change

Implementing the information security components will institute change in the Organization's processes and will influence the way people conduct their work. An important truth is that Organizations do not change, but people do, and therefore people change Organizations (Verton 2000). Information security changes in the Organization need to be accepted and managed in such a way that employees are able to successfully incorporate such changes into their work. As employees incorporate/internalize the information security components, their behavior will over a period of time become more acceptable in terms of protecting information assets. The change in behavior relating to compliance and the protection of information assets is important when the degree of success of the implementation of the components is to be measured.

2.5. Information security components versus Information security culture

The information security components are classified as follows:

2.5.1. Components that influence the organizational tier: sponsorship; strategy; governance; risk management; return on investment (ROI); legal and regulatory; policies, procedures; standards; guidelines; certification; best practice; change management. These components have an effect on how the organization operates and manages information security. Although each of these components in some way or other affect groups and individuals in the organization, they firstly serve to lay the foundation for defining how information security should be managed in the organization.

For instance, the strategy for information security will be based on the organizational strategy and risks identified in the environment. Again these components reside on an organizational tier, aiding to add formal structures and management for information security in the organization. In many ways the components categorized on this tier can be seen as the foundation for providing direction to groups of people and individuals in the organization in terms of protecting information.

2.5.2. Components that influence the group tier: program organization; monitoring and audit; compliance; trust; education and training; asset management; system development; incident management; technical operations; physical and environmental; business continuity management change management. The components categorized on the group tier mainly influence people as a group in the organization. For example, education and training are usually provided to employees in a group. Trust can relate to the trust that specific groups, departments or job levels have in terms of management protecting for instance personal information. Assets would need to be secured by departments. System development is conducted as part of a project consisting of team members or even different parties in the organization and more than one user would be affected by system changes. All employees in the organization need to follow the incident management process and a team of individuals could be responsible for the incident management and resolution process. Similarly, technical operations and controls would be deployed to all applications and environments, affecting more than one person.

2.5.3. Components that influence the individual tier: employee awareness; ethical conduct; privacy; change management. As mentioned earlier, the components can move between tiers and differ from one organization to the next. For instance, depending on the information security strategy, employee awareness might be conducted on a group tier as opposed to an individual tier due to huge staff numbers and cost constraints. It might not even be conducted at all. However, employee awareness is categorized on the individual tier as the individual is accountable for his/her behavior and compliance to the information security policy and requirements. Ethical conduct and privacy perceptions are seen as attributes of individuals which could vary between individuals and affect the manner in which they protect information assets.

Change management is categorized on the organizational, group and individual tier as any component that is implemented or changed on any of the tiers would result in change that needs to be managed appropriately.

As indicated above, an information security culture is cultivated on each of the three tiers of information security behavior. It is reflected in artifacts and creations, values and assumptions. For instance, an information security policy (policy component) is compiled on an organizational tier and gives direction to both management and employees regarding the protection of information assets. On a group tier, employees work together to implement the policy (program organization component), while on an individual tier employees are required to change their passwords every 30 days (employee awareness component). One of the outputs of a sound information security culture is strong password usage.

To summarize, an information security culture in the form of artifacts, values and assumptions develops for each component on each of the three information security behavior tiers. On the organizational tier, information security policy training sessions can be identified as an artifact that has resulted from the policy component. Values such as “I believe the information security policy is applicable to my daily duties” are gradually adopted. Employees visibly exhibit these values through compliance with policies or through management leading by example (mandating and maintaining a clean desk policy). Employees adopt basic assumptions such as “all employees comply with the information security policy” or, “if confidential information must be protected, I must save files in a secure location on the server”.

2.6. How to Assess an Information Security Culture

Limited information is available on how to assess an information security culture (Schlienger *et al*, 2005). The two approaches available are discussed briefly in the next paragraphs.

Schlienger and Teufel *(*2005) designed a questionnaire to obtain an understanding of the official rules supposed to influence the security behavior of employees. The researchers did not focus on the design of an information security culture framework that could serve as the foundation for developing an information security culture questionnaire (assessment instrument). They based their questionnaire on the three levels of organizational behavior of Robbins (2001), as well as on research work performed by Schein (1985) and subsequently developed information security statements relating to it. They performed substantive research to develop a decision support system for analyzing the results automatically and for enabling employees to complete the questionnaire online. They further aim to focus on extending the tool to allow benchmarking (2005).

Martins and Eloff developed a theoretical information security culture framework as the base for their information security culture questionnaire and the items to assess an information security culture. Their framework does not incorporate all the components that Schlienger and Teufel considered – for example, organizational culture levels. Furthermore, Martins and Eloff's information security culture questionnaire still needs to be validated (Da Veiga, 2008).

Other researchers like Kuusisto and Ilvonen (2003) did not perform extensive research on the assessment of an information security culture. They did not develop an information security culture questionnaire as such, but used ISO/IEC / IEC 17799:2000 (ISO/IEC 2000) as the base for their assessments (Da Veiga, 2008).

In the context of the above identified weaknesses in the approaches to assess information security culture Da Veiga proposed an approach that considers a comprehensive information security culture framework defined and presented under section 2.2 and an approach that uses the same framework as the basis of the instrument for assessing an information security culture and that organizations can apply to identify developmental areas and derive action plans whereby to render an information security culture conducive to the protection of information assets.

The proposed ISCF (information security culture framework) considers all the components required for information security culture, namely information security, organizational culture and organizational behavior. It integrates the aforementioned concepts to illustrate the influence between them. Because the information security components influence employees' information security behavior, an information security culture is cultivated visibly as artifacts and creations, values and assumptions. The ISCF illustrates not only what information security culture is, but also how the information security culture is cultivated and can be directed through appropriate governance of the information security components. The ISCF further defines what one should assess in order to determine the level of information security culture in an organization. It serves as the foundation for the design of a valid instrument to assess information security culture.

CHAPTER THREE
RESEARCH METHODOLOGY

This chapter covers research methodology; specifically the research design, the sources of data and sampling techniques adapted, the type of data that was used in carrying out the research, data collection instruments, data collection procedure, and data analysis methods.

3.1 Research Design

The study used a quantitative research method specifically survey research method in order to assess the information security culture at Development Bank of Ethiopia. Information security culture assessment model and instrument (A Questioner that uses a Likert Scale) were adopted from previous studies.

3.2 Population and Sampling Technique

The target population of the study were all employees of Development Bank of Ethiopia who operate and access the main core banking system called T-24 core banking system. The total number of employees operating and accessing the system were 403 employees (262 data inputers, 97 transaction authorizers, and 44 viewers) as of October 30, 2015 as per information obtained from Information technology process of the Bank. These employees were the actual employees of the bank that operate and have access to the system and would actually pose a threat to the information security of the bank.

The technique used in selecting the respondents was stratified sampling technique. Three stratum based on different privileges given to users (i.e. Data inputers, Transaction Authorizers, and Viewers) were formed. Finally proportionate sample were taken randomly from each stratum to make up the sample for the study.

Random sampling ensures the law of statistical regularity which states that if on an average the sample chosen is a random one, the sample will have the same composition and characteristics as the universe i.e. a representative sample (Kothari, 2004).

Stratified sampling: If a population from which a sample is to be drawn does not constitute a homogeneous group, stratified sampling technique results in more reliable and detailed information (Kothari, 2004).

$$n = \frac{N.z^2.p.q}{e^2(N-1) + z^2.p.q}$$

Where:

n is the required sample size

N is the population size, which is 403

p and q are the population proportions. p= 0.1 q=1-p

z is the value that specifies confidence interval when data is analyzed. Typical levels of confidence for surveys are 95%, in which case z is set to 1.96.

e sets the accuracy of sample proportions. e=5%

Hence, the sample size(n) with 5% precision and 95% confidence interval was 104 respondents. 65 % (68 staff) data inputers, 24% (25 staff) transaction authorizers, and 11% (11 staff) viewers. Overall 145 respondents were participated in the study which is more than the required sample size.

3.3 Types of Data and Instruments of Data Collection

Mainly Primary data was used in the study. The primary data was sourced from employees of Development Bank of Ethiopia through a structured questionnaire developed by Da Veiga (2008) and adopted by the researcher for this study. The required secondary data was not available in the Bank and hence its absence was used as one type of data input in the study.

3.4 Procedures of Data Collection

Primary data was collected through a self administered questionnaires distributed to respondents and collected by the researcher.

3.5 Methods of Data Analysis

Raw data was thoroughly edited, coded and utilized for analysis using Microsoft excel program. Major analytical statistics included frequencies and percentages while tables and pie chart were the basic methods for data presentation.

Descriptive analyses on the attitude and perception of the respondents on the major variables that determine the information security culture is presented. The Data collected is classified into categories and later establish the frequency in each category. The frequency of occurrence is presented in terms of percentages to have meaning.

Based on the findings, inferences and implications are drawn. In addition, the absence of secondary data is analyzed and the result is interpreted in a meaningful way.

3.6 Ethical Considerations

Ethics refers to moral principles or values that generally govern the conduct of an individual or group. Researchers have responsibilities to their profession, clients, respondents; and must adhere to high ethical standards to ensure that the interests of all stakeholders is adequately protected. All respondents in this study have participated in full consent and voluntarily. In addition utmost care is taken to protect privacy and anonymity of the respondents. The data collected from the respondents is used solely for this study and its objective thereof. Furthermore all works of other authors used in this study are duly acknowledged both in in-text citation as well as in the references section of the study. In analyzing and discussion of the collected data a high level of objectivity is pursued.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

This chapter includes the presentation, analysis and discussion of findings in accordance with the study objectives. Accordingly, the Biographical information of respondents is presented first followed by overall information security culture results and discussion of the results will follow.

4.1 Biographical Information of Respondents

Overall 145 employees participated in the study. In table 4.1, the first column shows Access Privilege Type, the second column shows number of respondents, and in the third column each access privilege type is presented as a percentage of the total respondents.

As indicated in table 4.1 below, 64% are data inputers, 24 % transaction authorizers, and 12% are Viewers on the core banking system.

Table 4.1: Respondents Access Privilege

Access Privilege Type	Number of Respondents	Respondents Percentage
Data inputer	93	64%
Transaction Authorizers	34	24%
Viewers	18	12%
Total	**145**	**100%**

In table 4.2 below, the first column shows experience of respondents in the Bank, the second column shows number of respondents and in the third column response of each group in terms of experience is presented as a percentage of the total respondents.

As presented in table 4.2, in terms of length of service only 10% of the participants have less than two years experience in the Bank, while 51% of the respondents have served in the bank between two and five years, and 39% of the respondents have more than five years work experience in the Bank.

Table 4.2: Respondents Experience in the Bank

Experience of Respondents in the Bank	Number of Respondents	Respondents Percentage
Less than 2 years	15	10%
Between 2 and 5 years	74	51%
More than 5 years	56	39%
Total	**145**	**100%**

4.2 Results and Discussions

4.2.1 Results

Primary Data Results for information security culture dimensions

For ease of analysis and interpretation the statements in the questioner were grouped under six dimensions based on the literature review done in chapter two and the number of respondents for each response in the questioner under the dimension were counted to make up the average result for their respective dimension. The respondents were further regrouped respondents with favorable attitude, respondents with neutral attitude, and respondents with unfavorable attitude. In order to obtain the respondents with favorable attitude, the strongly agree and agree responses were grouped together. The strongly disagree and disagree responses were grouped together to constitute respondents with unfavorable attitude.

In all table that follow, the first column is a serial number, the second column shows statements presented to respondents under leadership and governance dimension, the third fifth, seventh ninth, and eleventh columns shows the of frequency of respondents for each information security statement (question) in the dimension, and in the fourth, sixth, and eighth, tenth, and twelfth columns the strongly disagree, disagree, neutral, agree and strongly agree responses are presented respectively as a percentage of the total respondents for the statement.

Note: A: Agree; D: Disagree; N: Neutral; SA: Strongly Agree; SD: Strongly Disagree

Table 4.3 Result of Leadership and Governance Dimension

		SD	D	N	A	SA	Total Respondents
No	Statements	No (%)	No (%)	No (%)	No (%)	No (%)	No (%)
1	The protection of information is perceived as a top priority agenda by top management of the Bank.	5 (3.4%)	10 (6.9%)	8 (5.5%)	60 (41.4%)	62 (42.8%)	145 (100%)
2	Top Management in the Bank is committed to the protection of information assets.	3 (2.1%)	12 (8.3%)	10 (6.9%)	85 (58.6%)	35 (24.1%)	145 (100%)
3	I believe the Bank's Information security strategy supports the achievement of its business objectives.	7 (4.8%)	15 (10.3%)	6 (4.1%)	72 (49.7%)	45 (31%)	145 (100%)
4	I believe that the overall management process of information security in the Bank is adequate to protect information assets.	28 (19.3%)	30 (20.7%)	20 (13.8%)	58 (40%)	9 (6.2%)	145 (100%)
5	I believe the risk management processes of the Bank are adequate to identify risks such as the threat of viruses, hackers or natural disasters that could negatively impact on information security.	36 (24.8%)	61 (42.1%)	10 (6.9%)	18 (12.4%)	20 (13.8%)	145 (100%)
6	I believe that the Bank gets optimum value out of its critical information technology resources including applications, information, infrastructure, and employees.	38 (26.2%)	82 (56.5%)	2 (1.4%)	10 (6.9%)	13 (9%)	145 (100%)
Leadership and Governance-Overall Response		117 (13.4%)	210 (24.1%)	56 (6.4%)	303 (34.8%)	184 (21.1%)	870 (100%)

Source: Own Survey (2015)

In table 4.3 above, the overall response for leadership and governance shows 55.9% a positive attitude (21.1% of respondents strongly agree and 34.8% of respondents agree). More than 80% of respondents gave agree and strongly agree responses to statements like “The protection of information is perceived as a top priority agenda by top management of the Bank”; “Top Management in the Bank is committed to the protection of information assets”; and “I believe the Bank’s Information security strategy supports the achievement of its business objectives” which shows a positive attitude of respondents towards leadership and governance of information security of the Bank.

Table 4.4 Result of Security Management and Organization

		SD	D	N	A	SA	Total Respondents
No	Statements	No (%)	No (%)	No (%)	No (%)	No (%)	No (%)
1	There are adequate information security specialists/coordinators throughout the bank to ensure the implementation of information security controls.	86 (59.3%)	46 (31.7%)	8 (5.5%)	2 (1.4%)	3 (2.1%)	145 (100%)
2	I believe the Information security team adequately assists in the implementation of information security controls to protect information assets of the bank.	82 (56.6%)	47 (32.4%)	11 (7.6%)	1 (0.7%)	4 (2.8%)	145 (100%)
3	I believe the information technology process implements information security controls (e.g. restricting access to insecure areas, controlling access to computer systems, preventing viruses).	30 (20.7%)	65 (44.8%)	15 (10.3%)	12 (8.3%)	23 (15.9%)	145 (100%)
Security Management and Organization-Overall Response		198 (45.5%)	158 (36.3%)	34 (7.8%)	15 (3.4%)	30 (6.9%)	435 (100%)

Source: Own Survey(2015)

In table 4.4 above the overall result for Security Management and organization (45.5% of respondents strongly disagree and 36.3% of respondents disagree) shows by far the most unfavorable or negative dimension. 91% and 89% of respondents showed disagreement to statements like “There are adequate information security specialists/coordinators throughout the bank to ensure the implementation of information security controls” and “I believe the Information security team adequately assists in the implementation of information security controls to protect information assets of the bank” respectively, which contributed to the overall negative attitude responses for the dimension.

Table 4.5 Result of Security Program Management

No	Statements	SD	D	N	A	SA	Total Respondents
		No (%)	No (%)	No (%)	No (%)	No (%)	No (%)
1	I believe Employees should be monitored on their compliance to information security policies and procedures such as measuring the use of email, monitoring which sites visited and what software is installed on computers.	2 (1.4%)	3 (2.1%)	4 (2.8%)	86 (59.3%)	50 (34.5%)	145 (100%)
2	Action should be taken against anyone who violated restrictions on sites to be visited, usage of email, and software installed on computers .	1 (0.7%)	4 (2.8%)	6 (4.1%)	87 (60.0%)	47 (32.4%)	145 (100%)
Security Program Management-Overall Response		3 (1.0%)	7 (2.4%)	10 (3.4%)	173 (59.7%)	97 (33.4%)	290 (100%)

Source: Own Survey (2015)

In table 4.5 above the overall response for Security Program Management dimension shows the respondents attitude is the most favorable (33.4% of respondents strongly agree and 59.7% of respondents agree). More than 90% of Respondents have shown of agreement to both statements in this dimension which is also reflected in the overall responses for this dimension.

Table 4.6 Result of User Security Management

No	Statements	SD	D	N	A	SA	Total Respondents
		No (%)	No (%)	No (%)	No (%)	No (%)	No (%)
1	I receive adequate training to use the applications I require for my daily duties.	5 (3.4%)	10 (6.9%)	8 (5.5%)	64 (41.4%)	62 (42.8%)	145 (100%)
2	I am aware of the information security aspects relating to my job (e.g. when to change my password, which information I work with is confidential).	28 (19.3%)	30 (20.7%)	20 (13.8%)	58 (40.0%)	9 (6.2%)	145 (100%)
3	I have adequate knowledge about emergency procedures if I have difficulty in operating the system.	36 (24.8%)	61 (42.1%)	10 (6.9%)	18 (12.4%)	20 (13.8%)	145 (100%)
4	I accept responsibility towards the protection of information assets I use for my job.	13 (9.0%)	10 (6.9%)	2 (1.4%)	82 (56.6%)	38 (26.2%)	145 (100%)
5	I think it is important to regard the work I do as part of the intellectual property of the bank.	2 (1.4%)	2 (1.4%)	3 (2.1%)	80 (55.2%)	58 (40.0%)	145 (100%)
6	I believe that e-mail and internet access are for business purposes and not for personal use.	1 (0.7%)	4 (2.8%)	8 (5.5%)	58 (40.0%)	74 (51.0%)	145 (100%)
7	I believe that the Bank keeps private information confidential.	7 (4.8%)	15 (10.3%)	6 (4.1%)	72 (49.7%)	45 (31.0%)	145 (100%)
User Security Management-Overall Response		92 (9.1%)	132 (13.0%)	57 (5.6%)	428 (42.2%)	306 (30.1%)	1015 (100%)

Source: Own Survey (2015)

In table 4.6 above the overall result for User Security Management shows a positive respondents attitude (30.1% of respondents strongly agree and 42.2% of respondents agree). More than 80% of respondents have agreed with statements like “I receive adequate training to use the applications I require for my daily duties”; “I accept responsibility towards the protection of information assets I use for my job”; “I think it is important to regard the work I do as part of the intellectual property of the bank”; “I believe that e-mail and internet access are for business purposes and not for personal use”; “I believe that the Bank keeps private information confidential”; which contributed to the positive attitude of respondents to user security management dimension.

Table 4.7 Result of Technology Protection and Operation

No	Statements	SD	D	N	A	SA	Total Respondents
		No (%)	No (%)	No (%)	No (%)	No (%)	No (%)
1	I believe that the physical information assets I work with are protected adequately.	2 (1.4%)	3 (2.1%)	14 (9.7%)	86 (59.3%)	40 (27.6%)	145 (100%)
2	I believe that information security controls (e.g. access controls) of the application I use in my daily duties are adequate.	2 (1.4%)	9 (6.2%)	5 (3.4%)	82 (56.6%)	47 (32.4%)	145 (100%)
3	I believe the incident management process of the bank is effective in resolving information security incidents.	75 (51.7%)	56 (38.6%)	9 (6.2%)	2 (1.4%)	3 (2.1%)	145 (100%)
4	I believe the building I work in is adequately safe to protect information assets from threats such as burglary or flood.	1 (0.7%)	9 (6.2%)	18 (12.4%)	80 (55.2%)	37 (25.5%)	145 (100%)
5	I believe the bank will be able to continue its daily operations if there is a disaster (e.g. fire explosion or flood) resulting in the loss of computer system, people, and/or premises.	92 (63.4%)	35 (24.1%)	10 (6.9%)	4 (2.8%)	4 (2.8%)	145 (100%)
6	I know what to do in the event of a disaster resulting in the loss of computer system, people, and/or premises.	25 (17.2%)	85 (58.6%)	20 (13.8%)	12 (8.3%)	3 (2.1%)	145 (100%)
Technology Protection and operation –Overall Response		197 (22.6%)	197 (22.6%)	76 (8.7%)	266 (30.6%)	134 (15.4%)	870 (100%)

Source: Own Survey (2015)

In table 4.7 the overall responses for Technology protection and operation dimension shows that respondents have a negative or unfavorable attitude. (22.6% of respondents strongly disagree and 22.6% of respondents disagree). More than 75% of respondents have disagreed with statements like “I believe the incident management process of the bank is effective in resolving information security incidents”; “I believe the bank will be able to continue its daily operations if there is a disaster (e.g. fire explosion or flood) resulting in the loss of computer system, people, and/or premises” and “I know what to do in the event of a disaster resulting in the loss of computer system, people, and/or premises”; which contributed to the negative attitude of respondents to this dimension.

Table 4.8 Result of Change Dimension

No	Statements	SD	D	N	A	SA	Total Respondents
		No (%)	No (%)	No (%)	No (%)	No (%)	No (%)
1	I accept that some inconvenience (e.g. locking away confidential documents, making backups, or changing my password regularly) is necessary to secure information assets.	2 (1.4%)	7 (4.8%)	2 (1.4%)	84 (57.9%)	50 (34.5%)	145 (100%)
2	I am prepared to change my working practice in order to ensure the protection of information assets.	4 (2.8%)	8 (5.5%)	3 (2.1%)	83 (57.2%)	47 (32.4%)	145 (100%)
3	Changes to secure information assets are accepted positively in the bank.	3 (2.1%)	12 (8.3%)	10 (6.9%)	85 (58.6%)	35 (24.1%)	145 (100%)
Change Dimension-Average		9 (2.1%)	27 (6.2%)	15 (3.4%)	252 (57.9%)	132 (30.3%)	435 (100%)

Source: Own Survey(2015)

In table 4.8 the overall response show that Change dimension is the other of information security dimension where respondents attitude is the most positive. (30.3% of respondents strongly agree and 57.9% of respondents agree). More than 88% of respondents have agreed to the statements like “I accept that some inconvenience (e.g. locking away confidential documents, making backups, or changing my password regularly) is necessary to secure information assets” and “I am prepared to change my working practice in order to ensure the protection of information assets.”; which contributed to the overall positive attitude of respondents to change component of information security culture in the Bank.

Table 4.9 Result of Overall Information Security Culture of the Bank

No	Statements	SD	D	N	A	SA	Total Respondents
		No (%)	No (%)	No (%)	No (%)	No (%)	No (%)
1	Leadership and Governance	117 (13.4%)	210 (24.1%)	56 (6.4%)	303 (34.8%)	184 (21.1%)	870 (100%)
2	Security Management and organization	198 (45.5%)	158 (36.3%)	34 (7.8%)	15 (3.4%)	30 (6.9%)	435 (100%)
3	Security Program Management	3 (1.0%)	7 (2.4%)	10 (3.4%)	173 (59.7%)	97 (33.4%)	290 (100%)
4	User security management	92 (9.1%)	132 (13.0%)	57 (5.6%)	428 (42.2%)	306 (30.1%)	1015 (100%)
5	Technology protection and operation	197 (22.6%)	197 (22.6%)	76 (8.7%)	266 30.6%	134 (15.4%)	870 (100%)
6	Change	9 (2.1%)	27 (6.2%)	15 (3.4%)	252 (57.9%)	132 (30.3%)	435 (100%)
Overall Information Security Culture Result		616 (15.7%)	731 (18.7%)	248 (6.3%)	1437 (36.7%)	883 (22.6%)	3915 (100%)

Source: Own Survey (2015)

In table 4.9 above, the overall information security result shows 34.4 % overall negative attitude of respondents, 6.3 % neutral responses and 59.3% overall positive attitude. Security Management and organization (45.5% of respondents strongly disagree and 36.3% of respondents disagree) is by far the most unfavorable or negative dimension followed by Technology protection and operation dimension (22.6% of respondents strongly disagree and 22.6% of respondents disagree). The two information security dimensions where the employees attitude are the most favorable are Security Program Management (33.4% of respondents strongly agree and 59.7% of respondents agree) and Change (30.3% of respondents strongly agree and 57.9% of respondents agree).

Between the two extremes lie Leadership and Governance (21.1% of respondents strongly agree and 34.8% of respondents agree) and User Security Management (30.1% of respondents strongly agree and 42.2% of respondents agree)

Secondary Data Results

As per information gathered from the Bank's information technology process the bank has no a written and formal information security policy, guideline, procedure, and standards so far. Security policies, procedures, standards and guidelines dimension consists of the documented requirements defined by the organization, national, and international standards or guidelines to direct employee behavior. All statements (at least three statements) in the questioner aimed at assessing the attitude of employees regarding information security policy, guideline, procedure, and standards were excluded after learning the absence of such a written and formal document is lacking in the Bank. As a result the ideal result for this dimension is 100 percent unfavorable however it is not added up with the rest of the results for the other dimensions and is treated separately.

4.2.2 Discussion of the main findings.

Overall 145 employees of the Bank participated in the study which is more than enough sample to represent the population understudy. The participants represented users with different access privilege to the core banking system of the Bank with different service length in the Bank. 64% are data inputers, 24 % are transaction authorizers, and 12% are Viewers on the core banking system. The largest number of respondents had worked in the Bank for more than two years (90%) and 39% of the respondents have more than five year work experience in the Bank.

As presented in 4.9 above, 59.3 % of the respondents have a favorable attitude, 6.3% respondents have neutral attitude, and 34.4% respondents have unfavorable attitude towards the overall information security culture of the Bank. Therefore, the result shows that there is a positive aspect about the information security culture in the Bank in which the Bank can scale up its effort for a more conducive information security culture for the protection of its information assets. On the other hand a huge gap with respect to information security culture in the Bank is found (More than 40% of the respondents have either unfavorable or neutral attitude), which tells that the Bank needs to step up its effort to improve on some aspects of its information security culture given the sensitivity of the information security in banking industry.

Discussion on unfavorable Dimensions and Statements

Security policies, procedures, standards and guidelines dimension: One of the major findings of this study was the lack of a written and formal information security policy, guideline, procedure, and standards in the Bank. As per information gathered from the Bank's information technology process the bank has no written and formal information security policy, guideline, procedure, and standards so far. As a result all statements in the questioner aimed at assessing the attitude of employees regarding information security policy, guideline, procedure, and standards were excluded after learning the absence of such a written and formal document in the Bank. As a result the result for this dimension is treated as 100 percent unfavorable.

Security policies, procedures, standards and guidelines dimension consists of the documented requirements defined by the organization, national, and international standards or guidelines to direct employee behavior. ISO 17799 defines a policy as the "overall intention and direction as formally expressed by management". In other words, it is a document detailing what management expects of employees in terms of protecting information assets. According to Whitman and Mattord (2003), the objective of a policy is to influence the decisions, actions and behaviours of employees. It further specifies what behaviour is regarded as acceptable and what not.

Furthermore, policy is the foundation of the other information security components. Policy has a number of functions including setting standards and ensuring a minimum level of uniformity in implementation of information security components; providing a framework for action and for dealing with potentially sensitive security issues; and promoting the transparency and accountability among departments and employees.

Without information security policy, the appropriate direction for the other information security components such as the level of risk posed and the resultant level of protection required cannot be effectively provided. It is based on these risk definition and level of protection required that the organization can determine the organizational structure and resource to be committed for information security. Without an information security policy, security practices would be developed without clear demarcation of objectives and responsibilities among work units.

Effective information security policies would help to define the users' right and responsibility in relation to information within the organization and help users to understand acceptable and responsible behavior in information resources. The presence of well written and documented information security policy also helps senior managers to control and monitor employee behavior in relation to information resources. (Von Solms, 2000).

An example is an Information Security Policy stating that access should be controlled. A procedure provides the detailed steps of a component mentioned in a policy, for instance the process of granting access and distributing passwords. A standard details the minimum requirements, for instance that a password must be at least 8 characters long and consist of alpha-numeric characters. A guideline is a document that assists management in the implementation of information security.

Therefore, without information security policies and guidelines to direct and influence employee behavior, employees could well interact with information assets in ways that would introduce risk. In time, such potentially harmful behavior could unfortunately give rise to a culture where neglect is regarded as acceptable.

Security Management and organization (45.5% of respondents strongly disagree and 36.3% of respondents disagree), is by far the most unfavorable or negative dimension.

The objective in Security Management and organization dimension is to manage information security within the organization Program organization refers to the information security organizational design; composition and reporting structures (e.g., centralized or decentralized management of security). It also incorporates the roles and responsibilities, skills and experience, and resource levels committed to the organization security department (ISO 17799, 2005). The formal structures implemented by the organization influence employee attitudes and have an impact on their behavior (Robbins 2001: 325). A formal information security sponsor may be appointed on the organization's executive management. This appointment may influence employees to realize that it is important to invest time and money in information security. It could promote the value of responsibility from a senior level. Furthermore security management and organization should be based on the level of risk posed and the resultant level of protection required by the organization.

The unfavorable response regarding Security Management and organization shows that employees attitude that the organizational design, processes and procedures, composition of experts, skills and experience, and resource levels committed to the Banks information security are not adequate and effective. Employees become lenient in complying with the Banks requirement for information assets protection. Employees are not motivated to report information security incidents out of despair. Such unfavorable attitude towards security Management and organization of information security of the Bank undermine the effort of the Bank to nurture positive information security culture for the protection of information assets. Furthermore both statements in this dimension received the most unfavorable response. 59.3% of respondents strongly disagree and 31.7% of respondents disagree that there are adequate information security specialists/coordinators throughout the bank to ensure the implementation of information security controls; and 56.6% of respondents strongly disagree and 32.4% of respondents disagree that the information security team adequately assists in the implementation of information security controls to protect information assets of the bank.

Technology protection and operation: the second largest unfavorable dimension with 22.6% of respondents strongly disagree and 22.6% of respondents disagree that the bank has an efficient technological protection and operations system.

The technology protection and operations category relates to the traditional focus of information security. It involves the technical and physical mechanisms implemented to secure an IT environment (Von Solms, 2000). These include asset management, system development requirements, incident management, technical operations such as network security, and physical, environment, and business continuity controls. It is essential that the technology environment be monitored on a constant basis and that the risks of technology changes in the market be addressed (Von Solms, 2000).

Such unfavorable attitude towards the technology component of information security has a negative impact on the implementation and effective utilization of technology component of information security and hence affecting negatively the information security activity. Unfavorable specific statements in this dimension were further investigated to identify areas for intervention. The result reveals that 51.7% of respondents strongly disagree and 38.6% of respondents disagree that the incident management process of the bank is effective in resolving information security incidents. Incident management is the process used to identify, respond to and monitor information security incidents (ISO/IEC 17799:2005). An information security incident could be a virus affecting the organization’s network, a stolen laptop or sharing of a password between employees. The poor attitude of respondents regarding incident management process of the bank could be the result of weak internal help desk and information security organization of the Bank.

Furthermore 63.5% of respondents strongly disagree and 24.1% of respondents disagree that the bank will be able to continue its daily operations if there is a disaster (e.g. fire explosion or flood) resulting in the loss of computer system, people, and/or premises. Business continuity involves the prevention and mitigation of disruption, as well as the recovery of the business (processes, people and technology) from a disruption (ISACA 2008). A disruption could be a power failure or an earthquake affecting the LAN connectivity between offices. Disaster recovery is part of business continuity. Schiesser (2002) defines disaster recovery as “a methodology to ensure the continuous operation of critical business systems in the event of widespread or localized disasters to an infrastructure environment”. An organization has to identify its critical business systems and ensure that there is a plan in place to recover these systems. The plan could for instance involve another site where the environment is duplicated, and the making and off-site storage of such backups. The unfavorable attitude regarding the business continuity and disaster recovery process of the bank shows that the Bank does not have effective business continuity and disaster recovery plan in place.

Business continuity and disaster recovery plans are direct derivatives of the information security policy and their execution is closely related to the organizational design, processes and procedures, composition of experts, skills and experience, and resource levels committed to the Banks information security.

Moreover 26.2% of respondents strongly disagree and 56.6% of respondents disagree that the Bank gets optimum value out of its critical information technology resources including applications, information, infrastructure, and employees. This question is categorized under leader ship and governance dimension and the result reflect the overall assessment of employees with the Bank’s IT governance issue.

Discussion on favorable Dimensions and Statements

The two information security dimensions where the employees’ attitudes were the most favorable are Security Program Management and Change.

Security program management dimension: 33.5% of respondents strongly agree and 59.7% of respondents agree that they support the security program management activities like monitoring of the use of email, sites visited and software installed on computers. Monitoring and compliance as well as auditing are included in this category. It is essential to measure and enforce compliance of information security policy and guideline (Von Solms, 2000), and both technology and employee behavior (Vroom & Von Solms, 2004) should be monitored to ensure compliance with information security policies and to respond effectively and timely to incidents that are detected. Organizations need to evaluate their information security compliance level and they should have a mechanism to ensure that the practice of employees is compliant with the information security policy particularly because a significant number of information security breaches result from employee's failure to comply with security policies. As a result, policy enforcement is necessary and essential for the protection of information assets in an organization (Vroom & Von Solms, 2004).

Specifically 34.5% of respondents strongly agree and 59.3% of respondents agree that employees should be monitored on their compliance to information security policies and procedures such as measuring the use of email, monitoring which sites visited and what software is installed on computers and 32.4% of respondents strongly agree and 60% of respondents agree that action should be taken against anyone who violated restrictions on sites to be visited, usage of email, and software to be installed on computers.

Monitoring of employee behavior could include monitoring the installation of unauthorized software, the use of strong passwords or Internet sites visited. Technology monitoring could relate to capacity and network traffic monitoring. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organization (Vroom & Von Solms, 2004). As such the high positive attitude of employees towards security program management activities will lay fertile ground for the Bank in its overall effectiveness of information security protection endeavors.

Moreover statements employed to measure ethical attitude of employees reveal that 40% of respondents strongly agree and 55.17% of respondents agree that it is important to regard the work they do as part of the intellectual property of the bank; and 31% of respondents strongly agree and 50% of respondents agree that e-mail and internet access are for business purposes and not for personal use. The result shows that respondents are more inclined to ethical values and rules which is very conducive for favorable information security culture to thrive.

Change dimension: 30.3% of respondents strongly agree and 57.9% of respondents agree that they are willing to embrace change in order to protect information assets. Implementing information security components will institute change in the organization's processes and will influence the way people conduct their work. So the positive attitude towards change in the Bank will be useful to successfully implement and incorporate information security changes into their work. As employees incorporate/internalize the information security components, their behavior will over a period of time become more acceptable in terms of protecting information assets. An important truth is that organizations do not change, but people do, and therefore people change organizations (Verton 2000). The change in behavior relating to compliance and the protection of information assets is important when the degree of success of the implementation of the information security components is to be measured. In addition 34.5% of respondents strongly agree and 57.9% of respondents agree that they accept that some inconvenience (e.g. locking away confidential documents, making backups, or changing my password regularly) is necessary to secure information assets.

CHAPTER FIVE

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

This section of the report presents summary of the main findings of the study, conclusions, and recommendations.

5.1 Summary of the Main Findings

- The overall response for leadership and governance shows 55.9% positive attitude (21.1% of respondents strongly agree and 34.8% of respondents agree).
- The overall result for Security Management and organization (45.5% of respondents strongly disagree and 36.3% of respondents disagree) shows by far the most unfavorable or negative dimension.
- The overall response for Security Program Management dimension shows the respondents attitude is the most favorable (33.4% of respondents strongly agree and 59.7% of respondents agree).
- The overall result for User Security Management shows a positive respondents attitude (30.1% of respondents strongly agree and 42.2% of respondents agree).
- The overall responses for Technology protection and operation dimension shows that respondents have a negative or unfavorable attitude. (22.6% of respondents strongly disagree and 22.6% of respondents disagree).
- The overall response show that Change dimension is the other of information security dimension where respondents attitude is the most positive. (30.3% of respondents strongly agree and 57.9% of respondents agree).
- Overall 59.3 % of the respondents have a favorable attitude, 6.3% respondents have neutral attitude, and 34.4% respondents have unfavorable attitude towards the overall information security culture of the Bank.
- The Bank does not have a formal information security documents such as policies, guidelines, procedure, business continuity and disaster recovery plan.

5.2 Conclusions

From the study results and discussions made in chapter four, giving attention to the negative aspects, it can be concluded that:

- One of the major conclusions of this study is that the overall information security culture of the Bank is not conducive for the protection of information assets. There is no appropriate foundation for defining how information security should be managed in the Bank. The risk identification process and documentation as well as control mechanisms are unsystematic.

- The Bank does not have an information security policy and guideline that systematically coordinates the information security activities in the Bank as an organization, between departments, and individual employees. Hence, every member and department, information security activities, and information assets of the Bank are not effectively organized and directed towards the information technology purpose and achievement of the Bank Business goals and objectives. Consequently, the lack of proper information security policy and guideline implementation in the bank is a critical area of improvement.
- The Bank's Security Management and Organization is weak and not trusted and dependable by the Banks employees in its ability to provide assistance for effective information assets protection.
- Business continuity and disaster recovery plan of the Bank is not known and owned by the Majority of the employees.
- There is fertile ground in the Bank to implement any necessary changes regarding information security program.
- Employees of the bank would be very cooperative for Monitoring and compliance as well as auditing activities regarding information security.

5.3 Recommendations

1. The Bank should implement a comprehensive and adequate set of information security components that aid in addressing threats on the technical, process and people levels based on identified information security risks and the appropriate controls that are necessary to mitigate the identified risks. The Bank should adapt and implement International standards such as the Information Security Forum (ISF 2008), the Control Objectives for Information Technology (COBIT 2004), the Information Systems Audit and Control Association (ISACA 2008) and ISO/IEC 17799 (2005) to implement and manage information security components.
2. The Bank should compile and implement a formal well defined information security policy and its derivatives (guideline, Procedure and Standard) that give guidance and

direction to all members and stakeholders on the Bank regarding the management and protection of information assets. The policies should provide direction for the implementation of the other information security components and must be implemented in the organization by means of effective processes that also include awareness training, compliance monitoring and auditing thereof.

3. Executive Management of the Bank should organize information security department at a higher possible level in the organization and seriously take information security agenda as an important performance measurement and should commit enough resources for the operation of information security in the Bank.
4. The Bank should compile and implement a formal and well defined business continuity and disaster recovery document that give guidance and direction to all members and stakeholders on the Bank regarding the management and protection of information assets during disasters.
5. Finally, continuous information security culture development parallel with change in the business environment should be carried out in the Bank.

REFERENCES

Abiy,w. and Lemma,L. June 08, 2012. *5th ICT 2012 Ethiopia Conference. Information Security Culture in the Banking Sector in Ethiopia.* Venue: UNECA, Addis Ababa, Ethiopia

AIRC. 2008. *Attack Intelligence Research Center Annual Threat Report: 2008 Overview and 2009 Predictions,* Attack Intelligence Research Center, Alladin Knowledge Systems, Belcamp, MD (available online at http://www.aladdin.com/pdf/airc/ AIRC-Annual-Threat-Report 2008.pdf).

Borking, J. 2006. *Without privacy standards no trust in and outside cyberspace*. Retrieved online from https://www.primeproject. eu/events/standardisation-ws/slides/Withoutprivacynotrust-JohnBorking.pdf/file view

Brancheau, J. C., Janz, B. D., and Wetherbe, J. C. 1996. Key Issues in Information Systems Management: 1994-95 SIM Delphi Results, *MIS Quarterly* (20:2), pp. 225-242.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2004. "Economics of IT Security Management: Four Improvements to Current Security Practices," *Communications of the Association for Information Systems* (14), pp. 65-75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. 2009. "*Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers*," working paper, Sauder School of Business, University of British Columbia.

Chan, M., Woon, I. & Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior, *Journal of Information Privacy and Security*, 1(3), 18-42.

CobiT security baseline – An information security survival kit. 2004. USA: IT Governance Institute.

Da Veiga, A. 2008. *Cultivating and Assessing Information Security Culture*, University of Pretoria.

Deloitte and Touche LLP, 2004. *Perspectives on Internal Control Reporting.*

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

Dervin, L., Kruger, H. & Steyn, T. 2006. Value-focused assessment of information communication and technology security awareness in an academic environment. *In IFIP*

International Federation for Information Processing, Security and Privacy in Dynamic Environments, 201: 448-453.

Eloff, M., M., & Solms, S., H. (2000). Information Security management: A Hierarchical Approach for various frameworks. *Journal of Computer & Security*, 19(3), 243-256.

Ernst & Young. 2008. "Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey" (available online at http://www.ey.com/Publication/vwLUAssets/ 2008_Global_Information_Security_Survey_english/$FILE/20 08_GISS_ingles.pdf).

Furnell, S.M. 2004. Enemies Within: the problem of insider attacks. *Computer Fraud and Security*. 2004(July):6-11

Furnell, S.M. 2007. IFIP workshop- Information Security Culture. *Computer Fraud and Security*. 2007(26):35

Grant, R. 2005. Building a strong security culture. Retrieved online from http://www.citec.com.au/news/featureNews/2005/April/security_culture.shtml? Rate

Hall, E.M. 1998. *Managing risk: Methods for software systems development*. Reading: Addison-Wesley.

Hellriegel, D., Slocum, Jr. J.W. & Woodman, R.W. 1998. *Organizational behavior*. Eighth edition. South-Western College Publishing.

ISACA. 2008. *Information Systems Audit and Control Association*. http//:www.isaca.org.

Information Security Forum. 2000. *Information Security Culture- A preliminary investigation.* s.l.

ISO/IEC 17799 (BS 7799-1). 2005. *Information technology. Security techniques. Code of practice for information security management.*

Kothari C.R. (2004). *Research Methodology: methods and techniques*. New Delhi: India: New Age International (P) Limited.

Kruger, H.A. & Kearney, W.D. (2006). A prototype for assessing information security awareness. *Journal of Computers and Security, 25*, 289-296.

Kuusisto, R. and IIvonen, I. 2003. *Information Security Culture in Small and Medium Sized Enterprises*. Fronteirs of E-Business Research.

Lundy, O. & Cowling, A. 1996. *Strategic human resource management*. London: Routledge.

Martins, A. & Eloff, J. (2006). *Assessing Information Security Culture*. Johannesburg, South Africa: Rand Afrikaans University.

Martins, A. 2002. *Information Security Culture*. Johannesburg, South Africa: Rand Afrikaans University.

McCarthy, M.P. and Campbell, S. 2001. *Security Transformation*. New-York. MacGraw-Hill.

McIlwrath, A. 2006. *Information security and employee behavior*. Hampshire: Gower.

Pfleeger, C.P. 1997. *Security in computing*. Second edition. New Jersey: Prentice Hall.

Posthumus, S. & Von Solms, R. 2005. *IT Governance. Computer Fraud and Security*, 2005(6): 11-17.

PrinceWaterhouseCoopers. 2004. *Information security breaches survey*.

Robbins, S. 1998. *Organizational behaviour*. 8th edition. New Jersey: Prentice Hall.

Robbins, S. 2001. *Organizational behaviour*. 9th edition. New Jersey: Prentice Hall.

Robbins, S., Odendaal, A. and Roodt, G. 2003. *Organizational Behavior- Global and Southern African Perspective*. South Africa. Pearson Education.

Rotvold, Glenda (2008). *How to create a Security Culture in Your Organization*. Available at: http://content.arma.org/IMM/NovDec2008/How_to_Create_a_Security_Culture.aspx.

Schein, E.H. 1985. *Organizational culture and leadership*. San Francisco: Jossey-Bass Publishers.

Schiesser, R. 2002. *IT systems management*. Upper Saddle River: Prentice Hall.

Schlienger, T. & Teufel, S. 2005. Tool supported management of information security culture. *In IFIP International Information Security Conference (20th:2005: Makuhari-Messe, Chiba)*. Japan.

Schneier, B. 2000. *Secrets and Lies: Digital Security in a Networked World*, Indianapolis, IN: Wiley Publishing, Inc.

Schultz, E. 2005. The human factor in security. *Journal of Computers and Security, 24*, 425-426.

Sherwood, J., Clark, A. & Lynas, D. 2005. *Enterprise security architecture*. A business-driven approach. CMP Books: Berkeley.

Straub, D. W. 1990. Effective IS Security: An Empirical Study. *Information Systems Research* (1:3), pp. 255-276.

Tesseman, M.H. & Skaraas, K.R. 2005. *Creating a security culture*. Retrieved online from http://www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015-022.pdf

Verton, D. 2000. Companies aim to build security awareness. *Computer world*, 34(48): 24.

Von Solms, B. 2000. Information security – The third wave. *Computers and Security*, 19(7): 615-620

Von Solms, B. 2005. Information security governance – Compliance management versus operational management. *Computers and Security*, 24(6): 443-447

Von Solms, B. 2006. *Information security – The fourth wave. Computers and Security*, 25(2006): 165-168.

Vroom, C. & Von Solms, R. 2004. *Towards information security behavioural compliance*. *Computers and Security,* (23)3: 191-198.

Walton CB,R. and Walton-Mackenzie Limited. 2006. Balancing the insider and outsider threat. *Computer Fraud and Security*,2006(11):8-11.

Whitman, M.E. and Mattord, H.K. 2003. *Principles of Information Security*. Kennesaw State University.

Williams, P. A. (2009) What Does Security Culture Look Like For Small Organizations? *7th Australian Information Security Management Conference*, Perth, Western Australia.

APPENDIX

Appendix A

Questionnaires to Assess Information Security Culture of DBE

This questionnaire is prepared to collect data from DBE staffs to undertake assessment of information security culture of DBE. Specifically the data collected will be used for a thesis I am going to write for the partial fulfillment of Masters Degree in Accounting and Finance at St. Mary's University.

Whatever information is provided will be treated with utmost confidentiality and strictly will be used for academic purpose only. There is no need to write your name.

Thank you for taking the time to assist me in my educational endeavors.

Girum Ayalew

Mob. 09 23 28 56 09

Ext. 246

Biographical Data

1. Access privilege: Data inputer______ Transaction Authorizer_____Viewer ____________
2. Years of Service: Less than 2 years_ Between 2 and 5 years_____ More than 5 years___

Using the scale below, please indicate to what extent you agree or disagree with the statements relating to information security at Development Bank of Ethiopia.

SD= Strongly Disagree; D=Disagree; N=Neutral; A=Agree; SA=Strongly Agree

Statements		SD (1)	D (2)	N (3)	A (4)	SA (5)
Dimension 1: Leadership and Governance						
1	The protection of information is perceived as a top priority agenda by top management of the Bank.					
2	Top Management in the Bank is committed to the protection of information assets.					
3	I believe the Bank's Information security strategy supports the achievement of its business objectives.					
4	I believe that the overall management process of information security in the Bank is adequate to protect information assets.					
5	I believe the risk management processes of the Bank are adequate to identify risks such as the threat of viruses, hackers					

	or natural disasters that could negatively impact on information security.					
6	I believe that the Bank gets optimum value out of its critical information technology resources including applications, information, infrastructure, and employees.					
Dimension 2: Security Management and Organization						
7	There are adequate information security specialists/coordinators throughout the bank to ensure the implementation of information security controls.					
8	I believe the Information security team adequately assists in the implementation of information security controls to protect information assets of the bank.					
9	I believe the information technology process implements information security controls (e.g. restricting access to insecure areas, controlling access to computer systems, preventing viruses).					
Dimension 3: Security Program Management						
10	I believe Employees should be monitored on their compliance to information security policies and procedures such as measuring the use of email, monitoring which sites visited and what software is installed on computers.					
11	Action should be taken against anyone who violated restrictions on sites to be visited, usage of email, and software installed on computers.					
	Dimension 4: User Security Management					
12	I receive adequate training to use the applications I require for my daily duties.					
13	I am aware of the information security aspects relating to my job (e.g. when to change my password, which information I work with is confidential).					
14	I have adequate knowledge about emergency procedures if I have difficulty in operating the system.					
15	I accept responsibility towards the protection of information assets I use for my job.					
16	I think it is important to regard the work I do as part of the intellectual property of the bank.					
17	I believe that e-mail and internet access are for business purposes and not for personal use.					
18	I believe that the Bank keeps private information confidential.					
Dimension 5: Technology Protection						

19	I believe that the physical information assets I work with are protected adequately.					
20	I believe that information security controls (e.g. access controls) of the application I use in my daily duties are adequate.					
21	I believe the incident management process of the bank is effective in resolving information security incidents.					
22	I believe the building I work in is adequately safe to protect information assets from threats such as burglary or flood.					
23	I believe the bank will be able to continue its daily operations if there is a disaster (e.g. fire explosion or flood) resulting in the loss of computer system, people, and/or premises.					
24	I know what to do in the event of a disaster resulting in the loss of computer system, people, and/or premises.					
Dimension 6: Change						
25	I accept that some inconvenience (e.g. locking away confidential documents, making backups, or changing my password regularly) is necessary to secure information assets.					
26	I am prepared to change my working practice in order to ensure the protection of information assets.					
27	Changes to secure information assets are accepted positively in the bank.					