ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

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

By

Meheret Tesfaye Oda

ID No SGS/0047/2008A

Advisor: - Zemenu Aynadis (Asst. Prof.)

JANUARY, 2018

ADDIS ABABA, ETHIOPIA

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

BY

Meheret Tesfaye Oda

SGS/0047/2008A

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

JANUARY, 2018

ADDIS ABABA, ETHIOPIA

ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

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

BY

MEHERET TESFAYE ODA

SGS/0047/2008A

APPROVED BY BOARD OF EXAMINERS

Dean, Graduate Studies	Signature
Advisor	Signature
External Examiner	Signature
Internal Examiner	Signature

JANURAY 2018

DECLARATION

I declare that *ASSESSMENT OF INFORMATION SECURITY CULUTRE IN THE CASE OF COMMERCIAL BANK OF ETHOIPA* is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

Name	**Signature**

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

This thesis is dedicated to my parents and families for the inspiration they gave me during my studies.

Table of Contents

ACKNOWLEDGMENTS

First of all I would like to thank God and would like to give special thanks to my advisor Ato Zemenu Aynadis (Asst. Prof.) for always being there whenever I need help. The thesis would not have this shape without his professional inputs, criticism, guidance and support.

I would like to use this opportunity to thank the bank Information Security Managers and branch employees who took their time and respond to my questionnaires, and interview.

I would like to extend my thanks to all my families and friends for their support, encouragement and prayer not only during my thesis work but also all the way during my study.

LIST OF ABBREVIATIONS AND ACRONYMS

CBE: Commercial Bank of Ethiopia

ISM: Information Security Management

ICT: Information Communication Technology

ISC: Information Security Culture

IT: Information Technology

LIST OF TABLES

Tables **Page**

FIGURES

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 information security culture at commercial bank of Ethiopia. The study has employed descriptive research. The instrument (customized for the current study) incorporates statements that assess different issues in relation to information security by using 5-point Likert-scale questionnaire, distributed to employees and unstructured interview conducted with information security manager and selected through purposive sampling. To make the assessment Questioner were adopted from previous studies. A total of 257 questionnaires were filled and returned by employees. The analysis was made by making use of descriptive statistics. The empirical result shows that employee's level of awareness and knowledge towards information security is conducive and, the top management of the bank do commit enough time, money and people to protect information resource of the bank and also information security issues are not communicated and explained to employees as expected and information security controls and policies are applicable in CBE.

***Key words**: information security, awareness and knowledge, top management commitment, communication and explanation.*

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

Public and private organizations face a wide range of information threats. Securing their information has become a crucial function within the information system management regime. With an increasing reliance on technologies connected over open data networks, effective information security management (ISM) has become a critical success factor for public and private organization alike. In order to achieve effective ISM, it is essential to develop and deploy an effective information security culture. The application of information security culture assessment in the organization will help them to identify their strength and weakness with regard to information security. Herath and Rao (2009).From previous researchers it is noticed that the organizations especially private sector are not placing enough efforts in information security due to the high cost of information security. This is in line with the findings of Australian SME organizations. Also it is been noticed that the level of sensitivity and criticality of the organization business activities usually determines the level of efforts management paid to protect the information assets.

One of the major benefits of information security culture creation is the protection of the organization assets in which ultimately will have a "direct interaction with information assets and thereby minimize the threats that user behavior poses to the protection of information assets" (Da Veiga, 2008). The importance of creating a security culture within organization settings arises from the fact that the human dimension in information security is always considered to be the weakest link Therefore, the creation of an information security culture is necessary for effective information security management

Information is considered one of the most valuable assets to any organization Nowadays organizations operate in a global environment which enables organizations to collaborate and share information resources among themselves but at the same time exposes them to various threats both within and from outside of the organization. Therefore, it stands to a reason that organizations need to protect their information resources. A survey conducted by Price

Waterhouse Cooper in 2014 indicated that human errors are the most significant contributors to security incidents. Unfortunately, this “human error” factor has been generally neglected by many organizations who believe that technical controls will miraculously handle their security problems. As a result, a lot of time and money have been invested into technical tools and solutions to protect organizational valuable information assets while ignoring the “human factor” problem, which often is the very root cause of security breaches. The effectiveness of internal controls designed to protect the integrity, availability and reliability of information and information technology systems depends on the competency and dependability of the people who are implementing and using those (Kruger & Kearney, 2006). A measure that could be considered in order to reduce the risks posed by employees would be to focus on a security-aware culture (Ruighaver, Maynard, & Chang, 2007; Furnell, 2007). To manage their security risks, organizations must have a strong culture of security awareness. An information security culture is vital; and it should be implemented 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.Despite the fact, that many researchers have identified the importance and the need for an information security culture in organizations, few have established a clear and definitive meaning to the term “security culture”. Some authors see an information security culture as a goal to be achieved. For example, von Solms (2000) calls for the creation of a culture of information security within organizations, “by instilling the aspects of information security to every employee as a natural way of performing his or her daily job”. According to Martins and Eloff (2002b), 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 purpose of assessing that culture is to advance it to an adequate level. Assessing whether the information security culture is on an adequate level requires a value for it to be determined which isgenerally done through a quantitative assessment of the information security culture. An acceptable level of information security culture can be 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 information asset (Da Veiga, 2008). Assessment of information security culture assists an organization to identify the current and the desired information

security culture, the areas that need the most attention, and improvements needed to achieve the desired information security culture. According to Martins &Eloff (2002b) assessment in culture change can also help to ensure that recommendations from previous assessments are implemented. Conducting periodic assessments, implementing solutions and addressing the concerns arising from previous assessments can constantly improve the organization's information security culture. Another reason for culture assessment is to help an organization understand the behavior of its employees towards information security and to identify key issues for implementation and integration into the information security culture of the organization (Gebrasilase & Lessa, 2011).

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. CBE 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

- Attacks that shut the bank's branches system for hours
- Increased information security risks
- Information security law, ethics and relevant legislation and regulation concerning the management of information in the bank is not yet developed. Such problems damage the integrity, confidentiality and availability of the bank financial information and loss of customers' and stakeholders trust.

1.3 Research Questions

Based on the stated problems and review of related literature, this study assessed the following questions:

- Employee awareness and knowledge towards information security?
- The banks information security policy and controls in protecting information resources?

- Top management committeemen towards managing information security?
- Explanation and communication information security in the bank?

1.4 Objective of the Study

1.4.1 General Objective

The general objective of the study is to assess information security culture in Commercial Bank of Ethiopia.

1.4.2 Specific Objective

- To assess employee awareness and knowledge towards information security
- To assess if the bank has proper information security policy and security control in protecting information resources
- To assess explanation and communication of information security within the bank
- To assess top management commitment towards information security and adequate protection of information assets.

1.5 Significance of the Study

The relevance of this research work is of significant importance to Commercial Bank of Ethiopia. The research provides an insightful examination of information security culture in commercial bank of Ethiopia. Therefore this research improve information security culture of the bank thus, senior managers should adequately understand and be able to assess information security culture in CBE on betterment of their security culture. The student researcher believes that this study has the following significance. These are

- It enables the bank improve its information security culture.
- The information obtained can influence future management decisions, such as more awareness, training or resources allocations.
- It serve as way of raising awareness regarding information security and increase the commitment of employees as they feel that they are part of the process..
- Guide employees' security behavior in order to achieve a secure environment for organizational information assets.

- Identify key issue for implementation and integration of information security culture in the bank.
- As a “wake-up” call for management and to take decisive action.

Moreover, the result of the study provides additional research insight into how lack of information security culture affects the security of bank and inspires other researchers to conduct more researches in the area.

1.6 Scope of the study

The scope of the study is limited to information security culture assessment in the south district of Addis Ababa branch and information security management department in head office. The result of the research would be more comprehensive if it covers the entire CBE branches in Addis Ababa. However, due to financial and time constraints, it is delimited to head quarter and some sample branches in South Addis district. The head quarter is a place where major information security resources and facilities are performed. These staffs provide the necessary information about the study

1.7 Limitation of the study

The result of the research would be more comprehensive if it covers the entire bank and their branches in Ethiopia. However, due to financial and time constraints the student researcher has forced to focus on headquarters of sampled banks and another limitation of the study relates to lack of prior research studies on the subject which is considered relatively new to information security culture in Ethiopian, and to the banking sector in Ethiopia and also existence of limited awareness to information security. And also the sample size; the number of participants included in the sample may not be good representative of the population. This presents an important opportunity for other researchers interested in the subject to explore information security culture from other perspective. Future research is, therefore, recommended to address the above stated limitations.

1.8 Organization of the Study

The study consists of five chapters. Chapter one is the introduction chapter which presents background of the study, statement of the problem, research question, objective of the study, significance of the study, scope and limitation of the study. The second chapter deals with review of related literatures regarding the topic of the study. The third chapter discusses the research methodology and methods employed by the current study. Chapter four presents the data analysis results and their interpretation. Finally, based on the analysis and interpretation of the findings, chapter five presents the conclusion and recommendation.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

The purpose of this chapter is to provide an understanding of information security culture. This includes an introduction to information security culture. Before discussing information security culture, this study reviewed some security culture definitions.

2.1 Information Security Culture Definition

- An information security culture is defined Das 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 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)
- Information security culture is a subculture in regards to content. They declare: Security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee (Schlienger and Teufel, 2003).
- The totality of patterns of behaviors in an organization that contribute to the protection of information of all kinds (Dhillon,1995)
- Corporate information security culture that supports the information security policies, procedures, methods and responsibilities of the company, in such a way that information security becomes a natural aspect of the day to day activities of all employees of the company (Von Solms,2000)
- Information security culture is:
    - 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,

- The way people behave towards information security in the organization (Martin and Eloff's, 2002)

Many studies have shown that the establishment of an information security culture is necessary for effective information security (M. Eloff& von Solms, 2000; S. von Solms, 2000). What makes information security culture challenging is the complexity of defining and understanding both of the elements 'security' and 'culture'. Quantifying information security is challenging security culture reflects the values and beliefs of information security shared by all members at all levels of an organization (D'Arcy & Greene, 2009). Security culture covers social, cultural and ethical measures to improve the relevant security behavior of organizational members. It concentrates on a small aspect of human values and behaviors, and does not cover all the basic human values, norms and beliefs that influence organizational culture (Schlienger & Teufel, 2003).In addition, 'culture' itself is a complex concept in which difficult to measure. It has been argued that measuring security and culture is a complex process that will take significant time to investigate and is extremely hard to generalize to a large population As a result, the challenge faced is to quantify and investigate critical elements that conceptualize and measure security culture.

2.2 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.

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.

2.3 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. 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. 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.

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.

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 organizations business processes. 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.

2.4 Information Security Culture and Organizational Culture

Probably the best-known definition of organizational culture is "the way thingsare done here" (Lundy & Cowling 1996). Organizational culture can be seen as the personality of the organization (Robbins 2001) and it is the social glue that binds the members of an organization together. An organizational culture develops on the basis of certain activities in the organization, such as the vision of management and the behavior that employee's exhibit on an individual, group and organizational level (tier) (Hellriegel, Slocum & Woodman 1998; Robbins 2001). 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 CIS') (Schein 1985: 14). 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, Slocum &Woodman 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; Martins &Eloff 2002; Robbins; Hellriegel, Slocum & Woodman 1998). An information security culture is therefore

based on the interaction of employees with information assets and the security behavior they exhibit.

2.5 The Importance of Information Security Culture

The importance of an information security culture is also in its permanence. For such culture to be durable and to continue being effective, organizations also have to pay attention to the frequency of appropriate awareness campaigns, and how the message is communicated. Once a high level of awareness has been achieved and the right behavior is apparent within the organization concerning information security, follow-on effort may be less than in the initial movements, but cannot be zero. Times change, threats alter and, quite simply, people also forget. Continuing and visible management commitment to an information security culture, as well as correctly adapted levels of internal publicity and participation, are two axes along which an organization can continue to prevent information security problems and benefit from program payoffs. (Bosworth, Seymour & Kabay 2002).

2.6 Information Security Frameworks

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.

2.7 Information Security Components

2.7.1 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 2000), 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

2.7.2 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

2.7.3 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 risk such as the threat of virus, 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)

2.8 Managing Information Security Culture

Information Security Culture, like organizational culture, can't be created once and then be used all life time. To ensure that it corresponds with the targets of the organization and that the organizational members don't forget it, culture must be created, maintained or changed continuously. It's a never ending process, a cycle of evaluation and change or maintenance. The

first step is to analyze the actual Information Security Culture (pre-evaluation). If the culture doesn't fit with the organization's targets the culture must be changed. If it fits, it should be reinforced. The success of the actions taken must then be controlled (post-evaluation). This cycle is illustrated in the following figure. Schein, E. H. (1985).

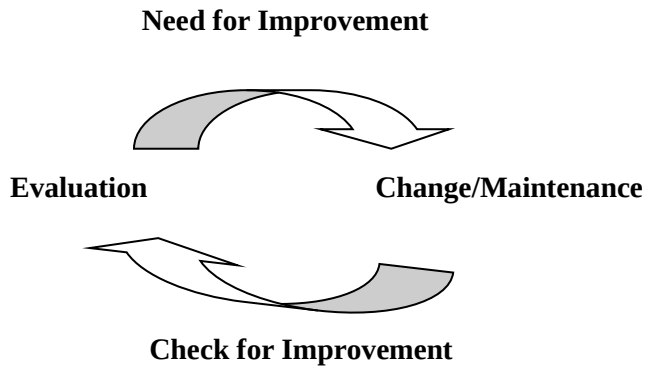

Fig 1.1 Information Security Culture Management Cycle

2.9 Information Security Culture Assessment Approaches

In order to minimize risks to information assets organizations need to ensure that an information security culture is introduced through education, training and awareness. To determine whether the information security is at an acceptable level, it needs to be measured by using an information security culture assessment instrument. The results from an assessment can be then used to highlight the areas in need for improvement in order to protect information assets (Da Veiga, Martins, &Eloff, 2007).The literature review indicated that there are only three research projects that provide an empirical research assessment instruments along with description of a process that can be used to assess information security culture, namely Martins and Eloff (2002b); Schlienger and Teufel (2005); and Da Veiga and Eloff (2010).

Martins and Eloff (2002b) used an assessment approach consisting of an audit process and including an information security culture questionnaire for the assessment of information security culture in an organization. Schlienger & Teufel (2005) used an information security culture management process incorporating a combination of methods for the assessment and management of information security culture in an organization. Da Veiga and Eloff (2010)

utilized an ISC assessment process through a survey including development of a questionnaire as an assessment instrument.

2.9.1 Assessment Approach by Martins and Eloff (2002b)

To determine whether information security culture is at an acceptable level in an organization, the researchers proposed an assessment approach consisting of an audit process. The assessment approach aims to determine employees' perceptions, attitudes, opinions and actions towards information security. From the analysis of the information gathered throughout the audit, organizations can address information security culture issues at the organizational, group and individual levels. The audit process consists of four phases:

- Phase 1: Development of the assessment instrument (questionnaire). The first phase outlines how to compile an information security culture questionnaire by considering the objective of the questionnaire and key issues of ISC in drafting the individual questions (e.g. not using jargon). Da Veiga, Martins and Eloff(2007) validated the proposed information security culture questionnaire by conducting an information security culture assessment in a financial organization and using the data to perform a factor and reliability analysis.
- Phase 2: A survey process that utilizes the questionnaire developed at phase one to assess the organization's information security culture; which entails the steps used to determine the sample population, the distribution and collection of the questionnaires and the completion of the survey. The researchers proposed this assessment to be a continuous process in order to promote information security culture in an organization by implementing and addressing the interpretations and recommendations from phase 4;
- Phase 3: This phase refers to the statistical analysis of the survey results obtained from phase two that gives a quantitative indication of the status of information security culture in the organization.
- Phase 4: This phase refers to interpretations of data analyzed during phase three. As a result, recommendations are made in order to address the identified areas of concern.

The survey process proposed by Martins and Eloff (2002b) focuses on the researchers' perspective to conduct an assessment of information security culture and not specifically of the

organization. However, management could still use the process as guidance when conducting an information security culture assessment.

2.9.2 Assessment Approach by Schlienger and Teufel (2005)

According to the researchers, information security culture needs to be maintained and modified continuously to ensure that it meets the organization's targets. This continuous process of analysis and change is referred to as the information security culture management process; and it involves four stages: diagnosis, planning, implementation and evaluation:

- Diagnosis*:* This stage analyses the existing information security culture and identifies any problems. This stage starts with a pre-evaluation of the information security culture in the organization in order to identify problems. According to the researchers, there are two aspects of analyzing information security culture: what to analyze (the assessment items); and how to analyze (the assessment methods). The assessment items may include information security documents such as information security policy of an organization. The researchers used a combination of methods to assess information security culture. A questionnaire was developed to determine the perceptions and attitudes of employees (true values), the perceptions and attitudes of the organization (official values), and what the employees think should be the best solution for each question. Unstructured interviews were conducted with the chief security officer and a technician responsible for security to get an overview of the information security; to interpret the results of questionnaires and discuss the results in terms of quality of received answers. Objective observation was also performed as part of assessing artifacts by comparing the respondent's answers with their behavior.
- Planning: This stage involves strategic and operative planning. Strategic planning is concerned with defining the clear targets or objectives for the development of information security culture (e.g. the information security policy); and identifying the market segments like employees, information technology staff and managers to segment the data for comparison. The operative planning involves internal communication in terms of awareness programs, training, education and management buy-in in order to promote the security awareness of employees and managers.

- Implementation*:* This stage refers to management commitment, communication with employees, providing education and training for employees to ensure their commitment. During this stage, detailed activities, responsibilities, resources, schedules and the budget need to be defined.
- Evaluation*:* This stage provides information regarding the efficiency and effectiveness of the implemented actions, which can help to improve the implemented actions and define necessary follow-ups.

Schlienger and Teufel (2005) provided a comprehensive approach that can help organizations to assess their information security culture and to address the areas identified for development by the assessment. It is structured and practical and can be used to guide the management of an organization, as they are required to conduct an information security culture assessment and follow up their findings with action plans.

2.9.3 Assessment Approach by Da Veiga and Eloff (2010)

Da Veiga and Eloff (2010) used the proposed information security culture framework (discussed earlier) to develop an instrument for assessing the information security culture in an organization. The researchers defined a process for conducting an information security culture assessment in an organization that consists of five steps:

- Information security culture assessment planning and preparation: This step includes the following actions: involving the stakeholders; developing an information security culture assessment instrument; validation of information security culture framework; determining population and sample size; conducting pilot study; and selecting an appropriate assessment technology (for example, a survey software, Survey Tracker, can be used to distribute, capture and conduct survey analysis);
- Information security culture assessment administration: The following step is concerned with distributing the questionnaires to the target population and obtaining the completed questionnaires back for analysis purposes. During this process a survey and its objectives are communicated to employees; the information security culture questionnaires are distributed in a preferred way(e.g. electronically or paper-based); and responses are tracked and monitored to ensure that a statistically representative response is obtained;

- Information security culture assessment data analysis: This step involves conducting a statistical analysis (for example, frequency distribution or standard deviation); determining validity of a questionnaire through the statistical analysis of its results (e.g. by utilizing the technique of structural equation modeling); and making sure the questionnaire used is reliable;
- Information security culture assessment report writing and feedback: The results and findings of the survey must be summarized in a report. Ideally, two report should be produced, one for managers and the other one for participant employees;

- Implement information security culture assessment action plans: As a result of information security culture assessment, actions plans for developing specific areas are identified that may include communicating information security concepts to employees, to explain the information security policy; or providing training and awareness programmes. These action plans could be incorporated into the organization's information security awareness programme. Certain revisions to the current information security awareness programme, induction training and communication material might need to be made. The progress of actions' implementation will need to be monitored. Over time, changes will start to emerge as employees' understanding of their roles towards information security improves, new recruits are trained efficiently to protect information assets and effective communication methods are used to convey information security messages. Eventually, the information security culture will also start to change. A following information security culture assessment can be conducted to determine whether the action plans were effective and had the desired effect on the information security culture. The results of the first and second assessment can then be compared for further insight. New action plans can again be identified and the cycle will continue.

Da Veiga and Eloff (2010) proposed an information security culture assessment process that can provide management with the steps to conduct an information security culture assessment, as well as the steps to validate the assessment instrument. This assessment instrument can be used in organizations to measure the prevailing information security culture. The results of the assessment can help the organizations to identify areas of development in terms of the information security culture, take corrective action and achieve the desired level of information

security culture. However, the ISC assessment process can be further improved by including qualitative research methods, such as interviews and observations.

2.10 Conceptual Framework

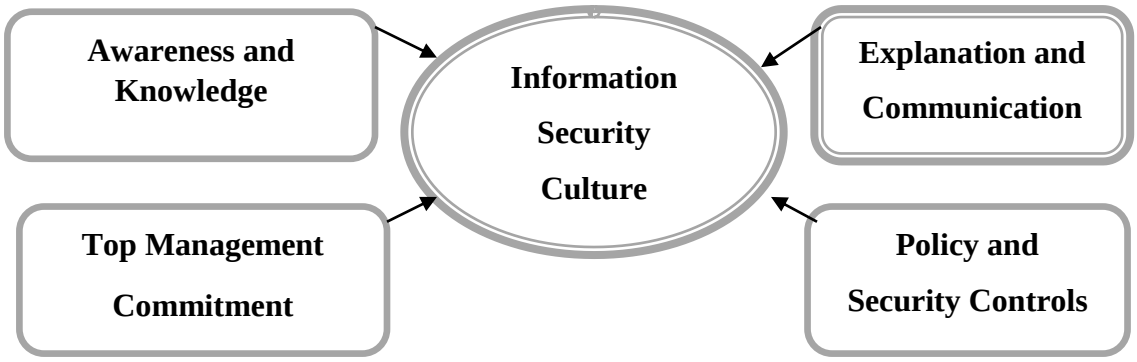

Figure 1.2 Research Conceptual Framework (ISACA 2008)

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter presents the research design and methodology. This includes the research design, sampling design and sampling technique, type of data, data collection method and procedure of data collection. At the end the method for data analysis is presented. The main aim of this research is to assess information security culture in CBE.

3.1 Research Design

A research design is the program that guides the researchers in the process of collecting, analyzing and interpreting the data. The researcher used descriptive form of research design in order to assess information security culture at CBE. The major purpose of descriptive research is to describe characteristics of a certain phenomenon. Descriptive research designs describe the characteristics of objects, people, or organizations C.R. Kothari, 2004. This research also attempted to give details on information security culture in CBE. The study was used of descriptive study to describe the data that the researcher got from the questionnaire and interview.

3.2 Population, Sample and Sampling Techniques

The researcher used the following sampling components: population, sampling techniques and sample size to prepare sampling design.

3.2.1 Population

The population of the study was 2,417 South Addis districts branch employees and ISM department team in head office. Among those, 2,417 South Addis district branches 300 employees from 15South Addis district branches were selected. And the researcher collected 15South Addis district branches' data and.

3.2.2 Sampling Technique

As a target populations of the study were CBE it is impossible and difficult to conduct the research on whole populations by student ability. So, the researcher selected representatives from

the populations to collect the data. To generalize the findings to the whole populations, the researcher used probability sampling method in which every district and branch has a chance (greater than zero) of being selected in the sample. Among probability sampling methods, simple random sampling (lottery method) technique is used to select sample districts and branches within the city. Similarly, to select employees like CSO (Customer Service Officers) and CSM (Customer Service Managers), the researcher implemented above stated sampling techniques. An unbiased random selection of individuals is important so that if a large number of samples were drawn, the average sample would accurately represent the population.

Additionally, to select special populations having in-depth knowledge and experience about the research questions, the researcher implemented no probability (judgmental or purposive) sampling techniques. In non-probability sampling, the researchers choose the sample based on who they think would be appropriate for the study. This is used primarily when there are a limited number of people that have expertise in the area being researched. Through no probability/purposive sampling method, the researcher select ISM department of CBE in Addis Ababa City Administration. The reason the researcher implemented purposive sampling technique; not using other sampling methods is those ISM teams are present only in Head Office of Commercial Bank of Ethiopia.

3.2.3. Sampling Procedures

The total number of CBE south Addis district branches employees has been taken from Commercial Bank of Ethiopia south district central office and using simple random sampling techniques branches having more than and equal to 20 employees are selected to be included in the sample this is done because since each branches employed different number of employees and is difficult to include all employees who are found in each branch after that purposive sampling technique was applied to information security mangers of sampled branches.

3.2.4 Sample Size

The sample size of this study is 300 employees which are found in 15 of south Addis district branches.

$n= \underline{N.z^2.p.q}$

$e^2(N-1)+ z^2.p.q$ Chapman and Hall/CRC, 2003.

Where:

n is required sample size

N is the population size which is 2,417

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 300 respondents.

3.3. Source

The study were gathered from branch employee and ISM department of the respective sampled banks, the primary data sources used in this study are IS Manager who have decision power related to Information security. This is because; ISM departments manage all the information security issues like information security standards, policy, procedures etc. In addition, data were gathered from branch employees like customer service office and customers service manager.

3.4 Instruments of Data Collection

Generally two types of instruments, namely questionnaire and interview were employed for the data collection. The primary data was collected through questionnaire (structured) and interview (unstructured) derived from Adéle da Veiga (2008) and adopted by the researcher for this study

3.5 Procedure of Data Collection

The data-gathering tool used in the study was drafted on the basis of the reviewed literature and the intended data to be collected. The set of questionnaires were distributed to the respondents. The data collection process was administrated by the student researcher. All interviews have been done by the student researcher. Data collections through interview were conducted by speaking to the respondents face to face. Before conducting the interview, the student researcher has tried to create conducive atmosphere and explain the purpose of the interview to them. As a

result necessary information was collected, organized and processed separately for interpreting and summarizing purpose to produce the major findings.

3.6 Method of Data Analysis

After collecting the raw data, classification and tabulation was done by the researcher to make it ready for the analysis. All collected data was organized and processed separately for each item in a way appropriate to answer the questions in the problem statement. Descriptive statistics was used to analyze the data by employing SPSS statics version 20 software. In addition to this statistical tool like tables, and verbal descriptions was used to present the data.

CHAPTER FOUR
RESULT AND DISCUSSION

The aim of the field study is to assess information security culture of CBE. Questionnaires and interview were used as instrument to carry out the study. The questionnaires were used to collect data about security issues defined by Adéle da Veiga. The result and discussion of each question in the surveyed branches is explained. The thesis research findings are classified into two major areas, findings from the interviews and findings from questionnaires

4.1 Respondent Information

The respondents of the research include Information Security manager who are engaged in managerial position and decision maker about Information security and IS team members and also officials at branch level who are Branch Manager, Branch Customer Service Office, Branch Customer Service Manager, Senior Customer Service Officer, Branch Auditor, Know Your Customer and Chief Casher.

Table 4.1 Demographic Information of Respondent

Gender	**Frequency**	**Percentage**
Male	162	63.0
Female	95	37.0
Total	257	100.0
Age	**Frequency**	**Percentage**
20-30	108	42.0
31-40	128	49.8
41-50	21	8.2
Total	257	100.0
Educational Level	**Frequency**	**Percentage**
Dip	1	4
Degree	173	67.3

Masters	81	31.5
PHD and above	2	.8
Total	257	100.0
Work Experience	**Frequency**	**Percentage**
1-3	146	56.8
4-6	81	31.5
7-9	20	7.8
10 and above	10	3.9
Total	257	100.0

Source: Survey Result 2017

The table given above describes the general findings regarding demographic status of the data. It tells that how dependent variables affects the independent. Based on the respondent's gender issue more participants' are male with 63%, while 37% of them are female. The bank has high demographic status as it shown in the respondents educational level, the respondents are 67.3 % first degree holder and 31.5% are second degree holders and 0.8% are PHD holder and also respondents found in the survey were experienced with 3.9% 10 years and above, 7.8% 7 to 9 years, 31.5% 4 to 6 years and 56.8% 1 to 3 years. Overall the result shows that the bank has enough level of experienced educated employees.

4.2. Analysis of Collected Data

4.2.1 Questioner

In this section, the results from data analysis are presented. The data analysis result is depicted using tables which refers employee's awareness and knowledge towards information security, policy and security controls, top management commitment, explanation and communication of information security. The result of the analysis is based on the response obtained from 15 branches. Findings of the questionnaire was summarized and attached hear in the following table bellow

Table 4.2 Information Security Awareness and Knowledge

Statements		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
I know what information security is	F	5	39	26	134	53	3.74	1.014
	%	1.9	15.2	10.1	52.1	20.6		
I know what my Responsibilities are Information Security	F	0	18	56	108	75	3.93	.888
	%	0	7.0	21.8	42.0	29.2		
I am informed of information security requirements to protect information	F	13	19	33	147	45	3.75	.997
	%	5.1	7.4	12.8	57.2	17.5		
I know what the risk are when opening e-mails from unknown senders, especially if there is an attachment	F	4	7	60	118	68	3.93	.863
	%	1.6	2.7	23.3	45.9	26.5		
I know how to use anti-virus software to scan for viruses (e.g when I download from the internet	F	30	9	51	132	35	3.52	1.139
	%	11.7	3.5	19.8	51.4	13.6		
When I leave my computer I always lock the screen	F	9	50	34	111	53	3.58	1.123
	%	3.5	19.5	13.2	43.2	20.6		
At the end of the day I ensure that there are no confidential documents left in my working area	F	2	13	52	109	81	3.99	.890
	%	0.8	5.1	20.2	42.4	31.5		
I understand the threats and vulnerabilities to information assets in my work environment	F	3	40	48	113	53	3.67	1.009
	%	1.2	15.6	18.7	44.0	20.6		

It is necessary that information security controls implemented in CBE are in line with best practice guidelines to secure information asset	F	26	26	11	115	79	3.76	1.270
	%	10.1	10.1	4.3	44.7	30.7		
It is necessary to commit money, people and time to protect information	F	4	36	10	98	109	4.06	1.079
	%	1.6	14.0	3.9	38.1	42.4		
It is important to take care when talking about confidential work related information in public places	F	30	1	5	146	75	3.91	1.173
	%	11.7	.4	1.9	56.8	29.2		
I believe that sharing of passwords should be used to make access to information easier	F	43	54	18	81	61	3.25	1.446
	%	16.7	21.0	7.0	31.5	23.7		
Some inconvenience (e.g locking away confidential documents, making backups or changing password regularly is necessary to secure important information	F	28	74	4	71	80	2.61	1.424
	%	10.9	28.8	1.6	27.6	31.1		
						Aggregated Mean	3.66	1.10

Source Survey Result 2017

In table 4.2 above the overall result for information security shows 1.9% of respondents strongly disagree,15.2% of respondents disagree,10.1% neutral,52.1% of respondents agree and 20.6% respondents strongly agree to the statement “I know what information security is”72.7% of employees are aware and knowledgeable towards what information security is, which showed the overall positive awareness and knowledge of employees towards information security. Since

information security is the protection of the confidentiality, integrity and availability of computerized data and system that process, maintain and report data during processing, and dissemination of output (kruger,2006)

7.0% of respondents disagree,21.8% of respondents are neutral, 42.0% of respondents agree and 29.2% respondents strongly agree to statements “I know what my responsibilities are regarding information security”.71.2% of employee knows their responsibility regarding information security which showed the overall positive awareness and knowledge of employees towards information security. If they know their responsibility and perform their daily job activities accordingly they can protect their information assets they work with.

5.1% of respondents strongly disagree,7.4% of respondents disagree,12.8% neutral, 57.7% of respondents agree and 17.5% respondents strongly agree to statements “I am informed of information security requirements to protect information” so that 74.7% are informed about information security which showed the overall positive awareness and knowledge of employees towards information security.

1.6% of respondents strongly disagree, 2.7% of respondents disagree,23.3% neutral, 45.9% of respondents agree and 26.5% respondents strongly agree to statements “I know what the risk are when opening e-mails from unknown senders, especially if there is an attachment” so that 72.4% know the risks, which showed the overall positive awareness and knowledge of employees towards information security.

11.7% of respondents strongly disagree,3.5% of respondents disagree,19.8% neutral, 51.4% of respondents agree and 13.6% respondents strongly agree to statements “I know how to use anti-virus software to scan for viruses (e.g when I download files from the internet” so that 65% know how to use anti-virus software, which showed the overall positive awareness and knowledge of employees towards information security.

3.5% of respondents strongly disagree,19.5% of respondents disagree,13.2% neutral and 43.2% of respondents agree, 20.6% respondents strongly agree to statements “When I leave my computer I always lock the screen” so that 63.8% lock their screen ,which contributed to the overall positive awareness and knowledge of employees towards information security.

0.8% of respondents strongly disagree, 5.1% of respondents disagree, 20.2% neutral, 42.4% of respondents agree and 31.5% respondents strongly agree to statements “At the end of the day I ensure that there are no confidential documents left in my working area” so that 73.9% ensure that no confidential documents are left in their working area, which showed the overall positive awareness level and knowledge of employees towards information security.

1.2% of respondents strongly disagree, 15.6% of respondents disagree, 18.7% neutral, 44.0% of respondents agree and 20.6% respondents strongly agree to statements “I understand the threats and vulnerabilities to information assets in my work environment” so that 64.6% of employee agreed to the statement, which contributed to the overall positive awareness level and knowledge of employees towards information security.

10.1 of respondents strongly disagree,10.1% of respondents disagree,4.3% neutral, 44.7% of respondents agree and 30.7% respondents strongly agree to statements “It is necessary that information security controls implemented in CBE are in line with best practice guidelines to secure information asset “so that 75.4% of employee agreed to the statement which showed the overall positive awareness level and knowledge of employees towards information security.

1.6% of respondents strongly disagree, 14.0%of respondents disagree, 3.9% neutral, 38.1% of respondents agree and 42.4% respondents strongly agree to statements “It is necessary to commit money, people and time to protect information” so that 80.5% of employee agreed to the necessity of committing money to protect information, which showed the overall positive awareness level and knowledge of employees towards information security.

11.7% of respondents strongly disagree,0.4% of respondents disagree,1.9% neutral, 56.8% of respondents agree and 29.2% respondents strongly agree to statements “It is important to take care when talking about confidential work related information in public places” so that 86% of employees agreed on the statement, which showed the overall positive awareness level and knowledge of employees towards information security.

16.7% of respondents strongly disagree, 21.0 % of respondents disagree ,7.0% neutral and 31.5% of respondents agree,23.7% respondents strongly agree to statements “I believe that sharing of passwords should be used to make access to information easier” so that 55.2% believed on sharing passwords, which contributed to the overall negative awareness level and knowledge of employees towards information security.

10.9% of respondents strongly disagree, 28.8% of respondents disagree, 1.6% neutral, 27.6% of respondents agree and 31.1% respondents strongly agree to statements “Some inconvenience (e.g locking away confidential documents, making backups or changing password regularly is necessary to secure important information.” so that 58.7% said it is necessary, which contributed to the overall positive awareness level and knowledge of employees towards information security. In general 3.66 mean value and1.10 standard deviation which means employees have good information security awareness and knowledge towards information security

As McIlwraith (2006) stated 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 and 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 towards information security.

Table 4.3 Top Management Commitment

Statements		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
Management in my business unit adhere to information security policy	F	0	21	59	98	79	3.91	.927
	%	0	8.2	23.0	38.1	30.7		
Senior management in CBE is committed to protect information asset of the bank	F	14	17	33	137	56	3.79	1.031
	%	5.4	6.6	12.8	53.3	21.8		
CBE pays adequate attention to an information security strategy in order to protect information	F	10	27	52	93	75	3.76	1.101
	%	3.9	10.5	20.2	36.2	29.2		
I believe CBE commits enough time,people,money to protect information	F	7	37	47	113	53	3.65	1.046
	%	2.7	14.4	18.3	44.0	20.6		
CBE complies with regulatory requirements relating to information security	F	14	11	52	78	102	3.91	1.139
	%	5.4	4.3	20.2	30.4	39.7		
						Aggregated Mean	3.8	1.04

Source Survey Result 2017

In table 4.3 above the overall result for top management commitment shows 8.2% of respondents disagree ,23.0% neutral ,38.1% of respondents agree and 30.7% respondents strongly agree to statements “Management in my business unit adhere to information security policy” so that 68.8% of agreed on the statement.

5.4% of respondent strongly disagree,6.6% of respondent disagree, 12.8% of respondents neutral,53.3% of respondents agree and 21.8% of respondent strongly agree to statements “Senior management in CBE is committed to protect information asset of the bank” so that 75.1% of respondent agreed on the statement.

3.9% of respondent strongly disagree,10.5% of respondent disagree, 20.2% of respondents neutral, 36.2% of respondents agree and 29.2% of respondent strongly agree to statements “CBE pays adequate attention to information security strategy in order to protect information’s, so that 65.4% of respondent agreed on the statement.

2.7% of respondent strongly disagree,14.4% of respondent disagree, 18.3% of respondents neutral, 44.0% of respondents agree and 20.6% of respondent strongly agree to statements “I believe CBE commits enough time ,people, money to protect information” so that 64.6% of respondent agreed on the statement.

5.4% of respondent strongly disagree,4.3% of respondent disagree, 20.2% of respondents neutral, 30.4% of respondents agree and 39.7% of respondent strongly agree to statements “CBE complies with regulatory requirements relating to information security” so that 70.1% of respondent agreed on the statement. In general 3.8 mean value and1.04 standard deviation which means top management are committed to secure information asset of the bank.

As stated in ISO 27001: role of top management and its importance written by JAY IMSZENNIK on Jan 15, 2016 The intent of involving top management within information security program is to ensure that enterprise governance is aligned with information security governance framework. Components of a well-designed information security governance program include leadership, structure, and processes designed to protect an organization’s information security assets.

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).

Table 4.4 Policy and Security Controls

Statements		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
CBE has written information security policy	F	27	16	50	130	34	3.50	1.129
	%	10.5	6.2	19.5	50.6	13.2		
CBE has written information security strategy	F	8	51	39	103	56	3.58	1.126
	%	3.1	19.8	15.2	40.1	21.8		
CBE has written information security standard	F	3	17	47	116	74	3.94	.916
	%	1.2	6.6	18.3	45.1	28.8		
Information security controls are adequately deployed in CBE to protect information	F	2	3	39	145	68	4.07	.729
	%	0.8	1.2	15.2	56.4	26.5		
The information security controls implemented by CBE support the business strategy	F	10	26	50	100	71	3.76	1.083
	%	3.9	10.1	19.5	38.9	27.6		
Threats to information assets are controlled adequately in my business unit	F	4	37	25	126	65	3.82	1.019
	%	1.6	14.4	9.7	49.0	25.3		
						Aggregated Mean	3.77	1.0

Source Survey Result 2017

In table 4.4 above the overall result for policy and security controls shows 10.5% of respondent strongly disagree,6.2% of respondent disagree, 19.5% of respondents neutral, 50.6% of respondents agree and 13.2% of respondent strongly agree to statements “CBE has written information security policy” so that 63.8% of respondent agreed on the statement. 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).

3.1% of respondent strongly disagree,19.8% of respondent disagree, 15.2% of respondents neutral, 40.1% of respondents agree and 21.8% of respondent strongly agree to statements “CBE has written information security strategy” so that 61.9% of respondent agreed on the statement. 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). 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.

1.2% of respondent strongly disagree,6.6% of respondent disagree, 18.3% of respondents neutral, 45.1% of respondents agree and 28.8% of respondent strongly agree to statements “CBE has written information security standard” so that 73.9% of respondent agreed on the statement.

0.8% of respondent strongly disagree,1.2% of respondent disagree, 15.2% of respondents neutral, 56.4% of respondents agree and 26.5% of respondent strongly agree to statements Information security controls are adequately deployed in CBE to protect information” so that 82.9% of respondent agreed on the statement.

3.9% of respondent strongly disagree,101% of respondent disagree, 19.5% of respondents neutral, 38.9% of respondents agree and 27.6% of respondent strongly agree to statements “The information security controls implemented by CBE support the business strategy” so that 66.5% of respondent agreed on the statement.

1.6% of respondent strongly disagree,14.4% of respondent disagree, 9.7% of respondents neutral, 49.0% of respondents agree and 25.3% of respondent strongly agree to statements “Threats to information assets are controlled adequately in my business unit” so that 74.3% of respondent agreed on the statement. The overall result found from the respondent information shows that CBE has information security policy and security controls. In general 3.7 mean value and1.0 standard deviation which means there is information security policy and controls in the bank.

As stated in ISO/lEC 27005 A systematic approaches to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS). This approach should be suitable for the organizations environment, and in particular should be aligned with overall enterprise risk management. Security efforts should address risks in an effective and timely manner where and when they are needed. Information security risk management should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operation of ISMS. Information security risk management should be a continual process. The process should establish the context, assess the risks and treat the risks using a risk treatment plan.

Table 4.5 Explanation and Communication of Information Security

Statements		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
The content of information security policy were effectively explained to me	F	21	143	3	53	37	2.77	1.273
	%	8.2	55.6	1.2	20.6	14.4		
Information security awareness initiative in CBE are effective	F	23	137	8	60	29	2.75	1.232
	%	8.9	53.3	3.1	23.3	11.3		
I received adequate training to use the application required for my daily duties to protect information	F	15	113	45	56	28	2.88	1.148
	%	5.8	44.0	17.5	21.8	10.9		
I am informed of information security requirements to protect information	F	46	80	9	82	40	2.96	1.405
	%	17.9	31.1	3.5	31.9	15.6		
						Aggregated Mean	2.84	1.26

Source Survey Result 2017

In table 4.5 above the overall result for explanation and communication of information security shows 8.2% of respondent strongly disagree,55.6% of respondent disagree, 1.2% of respondents neutral, 20.6% of respondents agree and 14.4% of respondent strongly agree to statements “The

content of information security policy were effectively explained to me" so that 63.8% of respondent disagreed on the statement

8.9% of respondent strongly disagree,53.3% of respondent disagree, 3.1% of respondents neutral, 23.3% of respondents agree and 11.3% of respondent strongly agree to statements "Information security awareness initiative in CBE are effective" so that 62.2% of respondent disagreed on the statement

5.8% of respondent strongly disagree, 44.0% of respondent disagree, 17.5% of respondents neutral, 21.8% of respondents agree and 10.9% of respondent strongly agree to statements "I received adequate training to use the application required for my daily duties to protect information" so that 44.9% of respondent disagreed on the statement.
17.9% of respondent strongly disagree, 31.1% of respondent disagree, 3.5% of respondents neutral, 31.9% of respondents agree and 15.6% of respondent strongly agree to statements "I am informed of information security requirements to protect information" so that 49% of respondent disagreed on the statement.

10.5% of respondent strongly disagree,0.8% of respondent disagree, 3.1% of respondents neutral, 55.6% of respondents agree and 30.0% of respondent strongly agree to statements "I am informed of information security requirements to protect information" so that 85.6% of respondent agreed on the statement. The overall result found from the respondent information shows that information security issues are communicated and explained to employees of the bank. In general 2.84 mean value and 1.26 standard deviation which means there is lack of information security explanation and communication in the bank

An awareness and training program is crucial in that it is the vehicle for disseminating information that user, including managers; need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise. today's financial sector must enforce an effective information technology security awareness and training program, proper rules of behavior for the use of online transaction IT systems and information flow need to be implemented. Employees first should be informed of

the expectations with regards to information security practices, but accountability must be derived from a fully informed, well-trained, and aware workforce (Wilson & Hash, 2003:7).

4.2.2 Interview

4.2.2.1 Top Management Commitment

As interview result found from information security department of CBE they said that involvement from top management is critical to the design and effectiveness of any information security program and CBE to protect its information asset the top management do commit enough time, human power and money.

And they also stated that the top management in CBE are committed and involve in information security programs like by

- Aligning information security with business strategy to meet the organization's strategic objectives.
- Creating risk management program that identifies and mitigates the impacts to an organization's resources and assets
- Allowing effective and efficient resource to secure information of the bank
- Reporting timely and useful information security metrics
- Giving initiatives to value-added information security issues

Security is ultimately the responsibility of all employees within an organization; however, the most successful information security programs demonstrate effective leadership from top management by setting a "tone at the top" and championing the importance of information security through well-designed policy and direction. The result can be an organization with information security ingrained as part of its culture.(Williams, 2009)

4.2.2.2 Explanation and Communication of Information Security

As interview result found from "Explanation and Communication of Information Security in CBE" they said that clear directives are being effectively and timely given to employees on how to protect sensitive (confidential) client information

They stated that failure to properly secure and protect confidential business information can lead to the loss of business/clients information in the wrong hands, confidential information can be

misused to commit illegal activity e.g. fraud which can in turn result in costly lawsuits for bank so since managing the security of information is our duty we working to give clear directives to employees on how to protect sensitive confidential client information.

And they also explained that information security policies are not explained to employees on time and they stated that though the banks internal website we are thinking to communicate and explain information security matters to employee of the bank.

4.2.2.3 Policy and Security Controls

As Interview result found from "information security controls of the bank such as security policy, standards, strategy "They said that Information security controls such as security policy, standards and strategies are in use and they also said that they support the business strategy of the bank and help the bank to protect its information asset and they also stated information security controls deployment in CBE line up with best practice guidelines to secure information assets and they also stated that holistic approach that is risk analysis is performed to control information security of the bank. Unless otherwise the bank perform risk analysis by viewing the whole picture based on its business interaction, security assurance may not be effective. Thus, the bank follow risk management process. These are: Information Assets Identification, Risk Identification, Risk Analysis, Risk Evaluation, and Risk control, Context Establishment, Risk Assessment, Risk Treatment, Risk Acceptance, Risk Communication and Risk Monitoring and Review.

CHAPTER FIVE

FINDINGS, CONCULUSIONS AND RECOMMENDATIONS

5.1 Summary of Findings

The major findings of the research shows as which is driven from both questioner and interview divided into four major parts information security and awareness of employees, top management commitment, explanation and communication of information security and policy and security controls.

- The overall response for information security awareness and knowledge of employees shows that they have good knowledge and awareness towards information security.
- The overall response of employees regarding top management commitment towards information security shows that the top management of CBE is committed to protect the banks information security.
- The overall response of employees regarding policy and security controls in CBE shows that there is a security policy and security controls in CBE.
- The overall response of employees regarding explanation and communication of information security issues in CBE shows that CBE doesn't communicate and explain information security issues to employees as expected.

5.2 Conclusions

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

- Employee's awareness and knowledge towards information security is good causing lower risks to the security of information assets.
- There is appropriate foundation for defining how information security should be managed in the bank. The risk management process and information security controls such as security policy, standards, strategy are organized and also the controls deployed in the bank line up with best practice guidelines to secure its information asset.

- Clear directives are not given to employees on how to protect sensitive (confidential) information by explaining and communicating information security policies and by informing employees about what is expected of them regarding information security
- The top management of the bank perceives information security as important and commits enough time, human power and money to protect CBE information asset.

5.3 Recommendations

- The bank to implement a comprehensive and adequate set of information security components that aid in addressing threats on technical, process and people levels basing its dynamic nature.
- The bank should compile and implement a formal well defined information security policy and its derivatives (guideline, procedure) 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 other information security components and must be implemented in the organization by means of effective process that also includes awareness training, compliance, monitoring and auditing.
- 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.
- The bank should improve the existing information security culture to bring adequate protection to information assets in the bank.
- Finally, continuous information security culture development parallel with change in the business environment should be carried out in the bank.

Reference

Bosworth, Seymour & Kabay, 2002.Computer security Handbook, fourth edition. New Jersey: Prentice Hall

Borking, J. 2006. Without privacy standards no trust in and outside cyberspace. Retrieved online from https://www.primeproject. eu/events/standardization-wsnslides/withoutprivacynotrust-johnborking.pdf/file view.

C.R.Kothari, 2004. Research Methodology Methods and Techniques. Former Principal, College of Commerce, University of Rajasthan, Jaipur (India)

Chapman and Hall/CRC, 2003. Binary Data.

Da Veiga, A. 2008. Cultivating and Assessing Information Security Culture. University of Pretoria, New Age International Publishers

Dhillon, G. 1995. Interpreting the Management of Information Systems Security. London School of Economics and Political Science, London

D'Arcy, J., & Greene, G. 2009. The Multifaceted Nature of Security Culture and Its Influence on End User Behavior. Paper presented at the IFIP TC 8 International Workshop on Information Systems Security Research, Cape Town, South Africa

Dervin, L., Kruger, H. &Steyn, T. 2006. Value-focused assessment of information communication and technology security awareness in an academic environment. In IFIP 54.

Da Veiga, A., & Eloff, J. H. P. 2007. An Information Security Governance Framework. Information Systems Management, 24(4), 361–372.

Da Veiga, A., &Eloff, J. H. P. 2010. A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196–207.

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

Gebrasilase, Temesgen&Lessa, Lemma Ferede. 2011. Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital, the African Journal of Information Systems: Vol. 3: Iss. 3, Article 1.

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

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

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

ISACA. 2008. Information Systems Audit and Control Association. (available online at http//:www.isaca.org.

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

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

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

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

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

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

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

Martins, A., &Eloff, J. 2002b. Assessing Information Security Culture. In ISSA (pp. 114).

Price Waterhouse Coopers. 2004. Information security breaches survey.

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

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

Ruighaver,Maynard & Chang. 2007. Organization Security Culture: Extending the end-user perspective. Computer and security, 26(1), 56-62.

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

Schlienger, T., & Teufel, S. 2003. Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. Paper presented at the DEXA Workshops.

Schein, E. H. (1985). Organizational Culture and Leadership: A Dynamic View. San Francisco,Jossey-Bass.

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

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

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

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

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

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

Von Solms, 2000. Information Security _The third wave. Computer and security, 19(7):615-620

Von Solms, B. 2006Information Security – The fourth wave. Computers and Security, 25(2006): 165-168 (Hall, 1998).

Williams, P. A. 2009 What Does Security Culture Look Like For Small Organizations7th Australian Information Security Management Conference, Perth, Western Australia.

Wilson, M. & Hash, J. 2003. Building an information technology security awareness and training program. Recommendations of the National Institute of Standards and Technology. 1st Draft, July 2002. Washington, DC: US Government Printing Office.

APPENDICES

Questionnaires to Assess Information Security Culture of CBE

Dear Sir/Mrs.

The researcher is doing a study on information security culture in CBE, in order to achieve that, the researcher designed a questionnaire; the questionnaire is intended to assess information security culture.

I believe that you are the best source to reach the required information and I hope to find cooperation from you through answering the questions contained in the thesis.

I appreciate your answers to this questionnaire and stress that you will be making a great effort to the research I make.

Best regards

Researcher

APPENDICES A: Questionnaire

Part I. Respondent Demographic Information

1. Gender_____
2. Age_____
3. Educational Level_____
4. Work Experience _____
5. Job Title_____

Instruction: Please put a "√"sign by choosing the scale provided below, please indicate to what extent you agree or disagree with the statements relating to information security at Commercial Bank of Ethiopia.

SD= Strongly Disagree

D=Disagree

N=Neutral

A=Agree

SA=Strongly Agree

No	Statements	SD (1)	D (2)	N (3)	A (4)	SA (5)
	Awareness and knowledge					
1	I know what information security is					
2	I know what my responsibilities are towards information security					
3	I am informed of information security requirements to protect information					
4	I know what the risks are when opening e-mails from unknown senders, especially if					

	there is an attachment.					
5	I know how to use anti-virus software to scan for viruses (e.g. when I download files from the internet					
6	When I leave my computer I always lock the screen					
7	At the end of the day I ensure that there are no confidential documents left in my working area					
8	I understand the threats and vulnerabilities to information assets in my work environment					
9	It is necessary that information security controls implemented in CBE are in line with best practice guidelines to secure information assts.					
10	It is necessary to commit money, time and people to protect information					
11	It is important to take care when talking about confidential work related information in public places.					
12	I believe that sharing of passwords should be used to make access to information easier.					
13	Some inconvenience (e.g. locking away confidential documents, making backups or changing password regularly is necessary to secure important information.					

	Top Management Commitment					
14	Management in my business unit adhere to information security policy					
15	Senior management in CBE is committed to protect information asset of the bank					
16	CBE pays adequate attention to an information security strategy in order to protect information					
17	I believe CBE commits enough time,people,money to protect information					
18	CBE complies with regulatory requirements relating to information security					
	Policy and Security Controls					
19	CBE has written information security policy					
20	CBE has written information security strategy					
21	CBE has written information security standard					
22	Information security controls are adequately deployed in CBE to protect information					
23	The information security controls implemented by CBE support the business strategy					
24	Threats to information assets are controlled adequately in my business unit					

	Explanation and Communication					
25	The content of information security policy were effectively explained to me					
26	Information security awareness initiative in CBE are effective					
27	I received adequate training to use the application required for my daily duties to protect information					
28	I am informed of information security requirements to protect information					

APPENDICES B: Interview

1) Is there any information security controls such as security policy, standards, procedures, guidelines, strategy that are deployed in CBE to protect information asset of the bank? If you answer is yes, do you think they support the business strategy of the bank?
2) Do you think information security controls deployed in CBE line up with best practice guidelines to secure information assets?
3) Is there clear directives given to employees on how to protect sensitive (confidential) client information and is there any training that is given to employees to control information security issues in order to protect information resource of CBE?
4) Does the top management of CBE perceives information security as important and commit enough time, human power and money to protect CBE information asset?
5) Is information security issues effectively explained to employee and adherence to information security enforced and take action against anyone who does not adhere to the information security policy?