ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION SECURITY MANAGEMENT FRAMEWORK FOR BANKING INDUSTRY IN ETHIOPIA

By

Kelemie Tebkew Yirdaw

June, 2013

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION SECURITY MANAGEMENT FRAMEWORK FOR BANKING INDUSTRY IN ETHIOPIA

A Thesis Submitted to the School of Information Science of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science

By

Kelemie Tebkew Yirdaw

Advisor

Mr. Workshet Lamenew

Addis Ababa, Ethiopia

June, 2013

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

INFORMATION SECURITY MANAGEMENT FRAMEWORK FOR BANKING INDUSTRY IN ETHIOPIA

By

Kelemie Tebkew Yirdaw

Approval by Board of Examiners

Chair: ---------- Signature: ---------- Date: ----------

Member: ---------- Signature: ---------- Date: ----------

Member: ---------- Signature: ---------- Date: ----------

June, 2013

DECLARATION

I declare that INFORMATION SECURITY MANAGEMENT FRAMEWORK FOR BANKING INDUSTRY IN ETHIOPIA 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.

---------- ----------

Signature Date

DEDICATION

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

ABSTRACT

Modern Banking increasingly relies on the Internet and computer technologies to operate their businesses and market interactions. Banks are on the way of using state-of-the-art technologies to increase efficiency and effectiveness in service delivery. However, these benefits do not come without risks for information being misused, service disrupted or any other attacks interrupting the normal operation of computer based information systems. The threats and security breaches are highly increasing in recent years globally. No exception for Ethiopia.

The objective of this study is to assess current Information Security Management (ISM) practices of banking sector, and to propose and develop ISM Framework. In this work, attempts were done to examine and compare the available ISM frameworks and best practices. This research combines ISO audit checklist and researcher's own experience to assess the information systems security practices in banking industry.

Both qualitative and quantitative research approach were used. Data were collected via questionnaire survey, document analysis, and interviews. To analyze the data SPSS tool is used. The study results show that surveyed banks are at diverse states in managing the security of their information systems. Moreover, they all are found to be at low level of ISM practice. A framework for ISM is developed and evaluated. The framework shows how banks identify their security requirements and select controls. Sixteen (16) main ISM domains are identified and in turn these ISM domains are classified under three categories viz. Administrative, Technical, and Physical & Environmental security. Further, some of areas that require policies and procedures are identified. Moreover, future research areas are also suggested to enhance the work.

Keywords

Information Security, Information Security Management, Information Security Management Framework, Threats, and Controls

ACKNOWLEDGMENT

Next to God, I would like to give special thanks to my advisor Mr. Workshet Lamenew, 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 surveyed Banks', IT security managers who took their time and respond to my questionnaires, and interview. I would like to say thank you all.

Last but not least, 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.

TABLE OF CONTENTS **Pages**

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ACRONYMS

ATM	Automatic Teller Machine
CBS	CORE Banking Solution
CCTV	Closed Circuit Television
COBIT	Control Objectives for Information and related Technology
EEPCOA	Ethiopian Electric Power Corporation Agency
ERM	Entity Relationship Model
FDRE	Federal Democratic Republic of Ethiopia
IDRBT	Institute for Development and Research in Banking Technology
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ISMS	Information Security Management System
IPS	Intrusion Prevention System
ISO	International Standardization of Organization
NBE	National Bank of Ethiopia
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PCIDSS	Payment Card Industry Digital Security Standards
RFP	Request For Proposal
SPPS	Statistical Product and Service Solutions
VMIA	Victorian Managed Insurance Authority

CHAPTER ONE

INTRODUCTION

1.1 Background

Information is an asset, which includes any organized documentation or data (in the form of hard or soft copy) incorporated into a communication structure that empowers the organization to have a better chance of reaching its goals (Benjamin, 2004).

As many scholars stated, information can be created, stored, destroyed, processed, transmitted, used (for proper & improper purposes), corrupted, lost, stolen and will be existed in the form of printed or written on paper, stored electronically ,transmitted by post or using electronics means, shown on corporate videos, displayed / published on web, verbal – spoken in conversations. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected (ISO/IEC 27001-2 & Fredrik, 2005).

In this world of information, managing information in an organization is very important. A bank that is good in information management is bound to be successful in this digital age. Information is key component in making a decision with the right and accurate information technology (Kei, 2004). In addition, Information is un-diminishable economic resource which is compared to the traditional asset like land, and capital. However, these benefits do not come without risks for information being misused, service disrupted or any other attacks interrupting the normal operation of computer based information systems. The threats and security breaches are highly increase in recent years globally. No exception for Banks in Ethiopia.

As such, ensuring the confidentiality, integrity, and availability of Information is vital to Banks. The customer information of Banks shall essentially be maintained in order to benefit from the competitive edge, profitability, legal compliance and commercial image. It is easy to imagine the consequences for a bank if its information was lost, destroyed, corrupted, burnt, flooded, sabotaged or misused. The effect of Security problems or breaches can lead to financial loss, Reputation loss, Intellectual property loss, Loss of customer confidence, Business interruption costs, and Legislative Breaches leading to legal actions .Generally, if a bank is hacked by someone it may cause loss of good will and at worst case it will collapse (Dancho, 2003).

In financial services industry, it is logical and right decision of investing on information security resources like: firewall, and Intrusion Prevention System (IPS) products (to protect the bank network,) and server level content blocking software (to prevent virus, malware, Spam…Etc.) to achieve the advantages such as customer trust and competitive advantage in turn to assure business continuity (Edward, 2011).

However, simply having best information security infrastructure without proper management may leave a bank with the best unavailable systems in the industry. Thus, the bank industry needs to pay close attention to how they manage the information security resources.

Information asset, like any other assets of a Bank, must be protected to ensure that the Bank's operation meets expectations, and there is no discontinuity in operations. However, securing information is both complex and challenging. The complexity stems from the universal and multi-functional nature of Information security, first, to protect Banks' valued assets, in order to achieve secure and reliable information assurance, and second, to advance business relations for the organization by creating platforms for trust, business alliance and collaboration. Further, the ever-growing dependence of Banks' on technology to drive businesses and to create a competitive advantage makes ISM for Banks' extremely challenging (Anon, 2009).

The other major challenge in Information Security in banking industry is the knowledge gap about the holistic approach of ISM. Due to this, most security requirements are derived by the external bodies than the Bank's management. Even though security measures are Technical, Physical and Human, Banks concentrate on the technical security measures only in order to comply with the external requirements. This situation creates bad security culture (Mohammed et al., 2009).

On top of that, globally, information security culture has a positive or negative impact in assuring information protection process in an organization. Thus, culture has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues. In addition, Information Security culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and considered to be a subculture of organizational culture. Literature in the area of security shows that research on information security culture is still in its early stages of development. Thus, the establishment of an organizational information security culture is necessary for effective information security (Mohammed et al., 2009).

Those ISM challenges in banking industry are numerous and inherently diverse. A traditional approach in addressing these challenges includes the use of technical controls to treat risks. While technical controls are helpful in protecting valued assets, unfortunately, technical controls alone are insufficient in providing reliable security. Thus, Global outsourcing, consumer-centricity, security compliance and legislation as emerging global business drivers have imposed new security requirements that complicate traditional perspective of ISM (Anon, 2009).

The majority of the research about ISMS has been performed by technologically leading countries such as the United States of America, the United Kingdom, the European Union and

Australia. On top of this, information security major international standards are written from a Western perspective, without knowing how applicable ISM concepts and practices to other cultures, which has different social, organizational, and security cultures, (Mohammed et al., 2009). As a result, there may be a need for extra or different considerations for ISM Implementation in banking sector.

Modern banking increasingly relies on the Internet and computer technologies to operate their businesses and market interactions. Banks are on the way of using state-of-the-art technologies to increase efficiency and effectiveness in service delivery (Philippa, 2004).

Lemma and Abiy (2012) stated that 'Information security awareness in the banking sector in Ethiopia is unsatisfactory. Consequently, the level of proper information security governance in the banking sector in Ethiopia is a critical area of improvement'. Thus, proper Information Security Management (ISM) and implementation that complies with local and international standards like Ethiopian Notional Information Security Policy, ISO27k series, and payment card industry digital security standards (PCI DSS) at organizational level is extremely crucial.

Ethiopian IT capacities are still in a developmental phase and are immature in relation to leading western technologically developed countries. In addition, the business environment of Ethiopian is different to the business environment in the USA and other Western countries (Mohammed et al., 2009).

As knowledge of the student researcher, therefore, this paper proposed ISM framework that can be used to guide the banking industry in developing and implementing ISMS. This was achieved: First, assessing the current practice of ISM process of banking industry in Ethiopia. Second, there is a need to define what ISM process is required from the globalization aspect. Finally, this paper answered the questions by developing ISM framework that guides the development and implementation of ISMS in banking sector in Ethiopia.

1.2. Statement of the Problem

Information system has become the heart of modern banking in our world today. The Banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy. In addition, the banking service has shifted from local branch banks to national and global presence and anywhere-anytime banking. The Banking business competition has motivated the advancement of services enabled by IT which in turn increased the information security risk. These threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the country (Patrick, 2011).

Technology has brought a paradigm shift in the functioning of banks and delivery of banking services. The growth of the internet, mobile, ATMs and communication technology has added

a different dimension to banking industry. Today, some of the transactions (balance, found transfer etc…) can be done from the comforts of one's home without visiting a bank's branch. This indicates that technology is no longer an enabler, but a business driver (IDRBT, 2011).

The Ethiopian Banks (both public and private) have been implementing comprehensive Banking software known as CORE Banking Solution (CBS) in accordance with the guidelines of the National Bank of Ethiopia (NBE). CBS helps each bank to acquire and implement state-of-the-art centralized banking application software that provides the needs of all branches of the Bank and its Head Quarter. According to the latest instruction issued by the NBE, it has become mandatory for all banks to be made CBS-compliant by the 30 September 2011 deadline. Further, as Federal Democratic Republic of Ethiopia (FDRE, 2011) stated the value and importance of information and information infrastructures has become conceived at national level since it is difficult to ensure peace, democratization and development without it. Moreover, to protect information, FDRE has published National Information Security policy even though it is focused mainly to compliant external standards.

Following this technology transformation and national information security policy in today's Ethiopian banking business, Information security becomes one of the key points for customer attraction, retention, and profitability. Thus, In order to get national and international competitive advantages, information like other assets must be properly managed from its creation up to disposal.

However, from Information security aspect, each Bank has applied some component of the comprehensive Information Security policy such as: Acceptable use policy for Computers and equipment, conventional key, backing up policy, "antivirus"… etc (source: researcher's experience and communication with IT experts who work in banking sector). In current state, many Banks have invested on IT security devices as part of CORE Banking Solution project. However, managing these IT security devices may be challenging since they do not have overall or comprehensive ISM framework which serve as a guide to develop and implement their own Information security policy based on their own requirement in line with notional information security policy (source: researcher's experience and communication with IT experts who work in banking sector).

As shown under section 2.5.1.5 below the most widely used international standard for information security management – sometimes called ISO27k series, is requirements oriented, meaning that it states the requirements organizations should satisfy if they want to undergo certification in accordance with the standard (Fredrik , 2005). However, the standard does not mention how this can be attained. Meaning, the standard does not clearly show the steps or methods that any Bank can follow in their requirement identification process when they develop ISMS. The proposed ISM Framework addressed this question.

Taking these facts in to consideration, in this study the student researcher assessed the current status and practices of ISM process in Bank industry in Ethiopia and proposed ISM framework which serves as a guide for developing and implementing ISMS in bank industry in Ethiopia. Thus, the study has the following objectives and questions.

1.2.1. Research Questions

a. What information security practices are employed in banking sector in Ethiopia?
b. What are the problems that impede the implementation of ISM System in banking sector in Ethiopia?
c. What are the success factors that have a great contribution for ISMS development and implementation process in banking sector in Ethiopia?
d. How Banks in Ethiopia identify their requirements prior to select best practices or controls?
e. Which ISM framework is widely used in the world, particularly in banking industry?
f. What kind of ISM framework is required in banking industry in Ethiopia?

1.2.2. General Objective

The major objective of this study is, to assess current ISM practices of banking sector, and to propose and develop ISM Framework which will work in banking industry in Ethiopia.

1.2.3. Specific Objectives

- Identify the ISM practices employed in sample Banks in Ethiopia.
- Identify the predominant problems that impede the ISM process in the banking sector in Ethiopia.
- Identify success factors that have a great contribution for ISMS development and implementation process in the banking sector in Ethiopia.
- Assessing different ISM frameworks which was done elsewhere in the world
- Developing ISM framework which works in the banking sector in Ethiopia.
- Evaluating the proposed ISM framework.

1.3. Significance of the Study

The student researcher believes that this study has the following significance for different parties. These are:

1. The result of this study shall serve as a guideline for those who are responsible for developing and implementing IS Policy in banking industry in Ethiopia.
2. It enables all banks to have a common ISM framework in Ethiopia.
3. The IT staffs could be able to get a better practice via a body of knowledge.

4. It may also serve as a starting point for practitioners and researchers who want to conduct more comprehensive research in this area from Ethiopian banking sector perspective.

1.4. Delimitation of the Study

The result of the research would be more comprehensive if it covers the entire Banks in Ethiopia. However, due to financial and time constraints, it is delimited to head quarter of some sample Banks in Addis Ababa. The head quarter is a place where major information security resources and facilities and the office of IT staffs are sited. These staffs can provide the necessary information about the study better than other staffs who work at branch level.

1.5. Limitations of study

The result of the research would be more comprehensive if it covers the entire Banks and their branches in Ethiopia. However, due to financial and time constraints the student researcher has forced to focus on headquarters of sampled banks.

1.6. Terms and Definitions

For the purpose of this thesis, the following terms and definitions apply.

- ***Availability*** - ensuring that authorized users have access to information when they need it.
- ***Asset*** -anything that has value to the bank
- ***Confidentiality*** - ensuring that access to information is appropriately authorized
- ***Information Security-*** is the preservation of Confidentiality, Integrity, and Availability of information.
- ***Integrity*** - safeguarding the accuracy and completeness of information and processing methods.
- ***Information Asset*** -All records, documents, data, and systems created, owned, or managed by the bank.
- ***Information security incident***-a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- ***Information asset Disposal-*** is a process of rejecting an electronic, paper, and physically recorded information assets.
- ***Security***- is the degree of protection against danger, damage, loss, and crime.
- ***Information privacy-*** is the ability of an individual or group to stop information about themselves from becoming known to people other than those they choose to give the information to.
- ***Risk***- A possibility that a threat exploits vulnerability in an asset and causes damage or loss to the asset.

- ***Threat***- Any circumstance or event with a potential cause of an unwanted incident, which may result in harm to a system or an organization.
- ***Vulnerability***- is a weakness of an asset or group of assets that can be exploited by one or more threats.

1.7. Organization of the Thesis

This study is organized in six chapters. These are:

Chapter One: introduces what an ISMF is and the status of security from banking industry and Ethiopian scenario. This chapter also presents the statement of the problem and the objective of the study.
Chapter Two: is the part where literature on information security, information asset, threats, computer security evolution, information security management, information security management frameworks (standards), ISM Framework developing methodologies was reviewed and presented for further description of the research area. Further related works are presented.
Chapter Three: this chapter presented research design and methodology which includes general insight on the existing research methods, what research method was employed in this thesis and why? Selection of sample for the study, data collection techniques, and data analysis methods was stated clearly.

Chapter four: is where the data collected through questionnaire, interview, and document collection was analyzed and presented. And the findings from the analysis were discussed, interpreted and summarization was made as related to the research problems statement.
Chapter five: is the part where a new proposed ISM Framework clearly presented.
Chapter six: concluding remarks and recommendations were made. And future possible study areas were also suggested.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

In this chapter, the student researcher has tried to review the background of Information Security Management and its theoretical and empirical framework for designing and implementing ISMS in a bank. The reviewed points are: Information and security, information asset, Evolution of Computer Security Strategies, information security, information security management, information security management system, information security management framework, information security threats, risk assessment, the three big ISMS designing and implementing standards, comparison made based on 11 benchmarks, which standard comes first, the more appropriate standards for banking sectors, ISM and its organization structure, ICT profile and standards in Ethiopia, methodologies, and research design approach and steps used by other scholars in developing ISM framework.

2.1. Information and Security

Information and security are two sides of a coin. Information is any organized documentation or data whether in hard copy or soft copy. Whereas the term Security is to make safe or secure information assets as defined by (ISO/IEC27001-2, 2005). In addition, as stated by Mohan and ISO27k Implementers' forum (2012) security encompasses People, Process and Technology and not only devices. People who use or interact with the information; the processes refer to "work practices" or workflow and the repeatable steps to accomplish business objectives, and Technology "what we use to improve what we do".

As many scholars stated, information can be created, stored, destroyed, processed, transmitted, used (for proper & improper purposes), corrupted, lost, stolen and will be existed in the form of Printed or written on paper, stored electronically ,transmitted by post or using electronics means, shown on corporate videos, displayed / published on web, verbal – spoken in conversations. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected (ISO/IEC 27001-2 & Fredrik, 2005).

The ever increasing use of electronic channels by customers, information security is becoming complex. The occurrence of security breach is not if, but when. Thus, it needs an appropriate information security management structure to achieve bank's objectives.

2.2. Information Asset

As defined in ISO/IEC 27001-2 (2005) "Asset is anything that has value to the organization". Information is an asset for a bank since it has value. In addition, Information is a key strategic

and operating asset for many enterprises and more particularly for financial services industry like banks. Its reliability, accuracy and availability are critical to achieve business goals. From a customer perspective, privacy and confidentiality needs protection (IDRBT, 2011).

Information system has become the heart of modern banking in our world today, and information has come to be the most valuable asset to protect from insiders, outsiders and competitors. Customers are very concerned about privacy and identity theft. Business partners, suppliers, and vendors are seeing security as the top requirement, particularly when providing mutual network and information access (Munirul et al., 2011).

Accordingly, banks must understand not only their physical assets, but also their information assets and where they keep their most valuable and sensitive information and equipment. Physical assets, such as servers and workstations, are more easily tracked and protected. Data may be more difficult to track, but to protect it; banks must understand the types of data they process, where they process it, and where they store it (George et al., 2012). Therefore, it is useful to begin by promoting a culture that recognizes the value of information as bank asset. Top managements need to set the tone and security posture by establishing security vision and strategy (IDRBT, 2011).

The best way for a bank to know its assets and protect them from attack, including from insiders, is to conduct a risk assessment. A risk assessment will teach a bank about the types of data its systems process, who uses the data, and where it is stored (George et al., 2012).
According to NIST (2012), the risk assessment framework includes six steps. Each of these steps requires the bank to understand its assets. Key questions that must be answered before the bank can move forward with a protection strategy include the following:

- What types of data are processed?
- What types of devices process this data (servers, workstations, mobile devices, etc.)?
- Where the data is stored, processed, and transmitted (single location, geographically dispersed, foreign countries, etc.)?

Answering these questions will help the bank inventory the data and systems that need to be protected from various attacks.
Physical inventories of equipment and the data they host will help the bank to identify critical assets. There are two methodologies for creating a complete inventory: service based and hardware based (George et al., 2012). Some banks may have a service catalog, rather than a conventional inventory, that contains the information services the bank needs to fulfill its mission.
A service-based inventory establishes a hierarchy of assets, starting with a top-level service, branching into the information assets that support it, branching again into the assets that support them, and so on.

A basic walkthrough of a data center is a tedious yet effective method of collecting hardware information for an inventory. However, hardware itemization does not constitute a complete inventory. Banks need to work closely with system administrators to become fully aware of the logical assets contained within each piece of hardware and add their business owners' contact information (George et al., 2012).

2.3. Evolution of Computer Security Strategies

As Anene and Annette (2007) stated that before computer security evolved into its various dimensions of today, the primary security focus of most organizations was in physical protection of their assets. Gradually, the rapid growth of computer networks and the advent of the Internet added another dimension to information security.

Time Frame	State of Affairs Security	General Location of Computers	Security Objectives	Security/Strategy Methodology
Up to early 1980s	Computers used simply as business tools to automate business processes	Computers located in computer centers	Securing computer centers	Accomplished through physical security
Up to early 1990s	Computers used throughout the enterprise (Distributed use of computers)	Computers located throughout the organization	Securing IT systems and networks	Through software residing on IT systems
Early 2000s to Present	IT systems supporting information as business assets	Computers located within and outside the enterprise	Securing business information systems	Through information security management

Table 2.1. Adopted from (Anene & Annette, 2007)

Over the years, as Anene and Annette (2007) stated and other many scholars agreed that the focus of information security evolved from physical security of computer centers to securing information technology systems and networks, to secure business information systems. With the Internet (like Internet & Mobile Banking), computers can communicate and share information with other computers outside bank's network. This meant that the existing security model was inadequate to meet the threats and challenges inherent in this new

technology services. A new approach to information security management is needed to meet these security challenges.

2.4. Information Security and Risk assessment

2.4.1. Information security

The definition of information security varies across scholars and/or institutes since it does not reach in its maturity level due to technological evolution. As a result many scholars define information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. In addition, Anene and Annette (2007) define information security as "…the Application of any technical methods and managerial processes on the information resources (hardware, software, and data) in order to keep organizational assets and personal privacy protected."

On the other hand, Fredrik (2005) defines information security as "…protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities."

However, a broad and internationally recognized definition of information security is given in ISO/IEC 17799 standard as "The preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods), and availability (ensuring that authorized users have access to information and associated assets when required) of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (Anene & Annette , 2007).
This definition of information security will be used as reference in this paper because it is more comprehensive and suitable for this research work.

2.4.2. Information Security Management

Information Security Management (ISM) is the process of protecting electronic and non-electronic information assets against the risks of loss, misuse, damage, and disclosure or corruption (ISO27001-2, 2005).

According to Fredrik (2005), "Information Security Management is the management of information security in organizations". Hence, the concept denotes those activities in the bank related to the direction and control of the security over information assets. Activities include (e.g.) assessment of threats and the current state of information security in the bank, design and implementation of administrative (information security rules for employees, etc.) and technical (access control systems, etc.) security controls, and operation of the day-to-day

efforts to preserve information security (documentation of and response to incidents, training of employees, etc.).

As Anene and Annette (2007) defined "information security management refers to the structured process for implementation and ongoing management of information security in an organization".
As you can see from the above definition the management and the structure of IT department within the bank has a great contribution in information security management. The generalist approach is prone to attack, employees' dissatisfaction, as a result turnover also increases.

2.4.3. Information Security Management System

As Fredrik (2005) defined an Information Security Management System (ISMS) is a controlled approach to manage sensitive company information so that it remains secure. It encompasses people, processes and IT systems. The function of ISMS is to verify and control risk and manage all information systems security efforts in the organization.
In addition, Mohan and ISO27k Implementers' forum (2012) stated that the ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

Further, The definition of the ISMS itself is given by ISO/IEC 27001-2 (2005) that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Regulations and various privacy / data protection policy impose a number of obligations to banks. Meanwhile viruses, worms, hackers, phishers and social engineers threaten banks on all sides. Hackers are likely to cause huge losses for the bank such as by theft of customer data, spy on business strategy, for the benefit of competitors.

Therefore, it is imperative for banks to use ISMS to effectively manage their information assets. ISMS basically consists of sets of policies put place by the banks to define, construct, develop and maintain security of their computer based on hardware and software resources. These policies guide the way in which computer resources can be used. Furthermore, ISMS is the organizational infrastructure (it is not a computerized system) that enables information to be shared, whilst ensuring the protection of information and information processing assets (Fredrik, 2005).

2.4.4. Information Security Threats

A threat is any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats generally can be classified as Natural and Deliberate or Accidental. These threats, as stated by Michael (2003), include:

- Act of Human Error or Failure (accidents, employee mistakes)
- Compromises to Intellectual Property (piracy, copyright infringement)
- Deliberate Acts of Information Extortion (blackmail of information disclosure)
- Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)
- Deliberate Acts of Theft (illegal confiscation of equipment or information)
- Deliberate Software Attacks (viruses, worms, macros, denial of service)
- Forces of Nature (fire, flood, earthquake, lightning)
- Quality of Service Deviations from Service Providers (power and WAN service issues)
- Technical Hardware Failures or Errors (equipment failure)
- Technical Software Failures or Errors (bugs, code problems, unknown loopholes)
- Technological Obsolescence (antiquated or outdated technologies)
- etc.

In addition to this, technically specking the following major categories will be the cause of information system threats: Malware, Malicious insiders, Exploited vulnerabilities, Careless employees, Mobile devices, Social networking, Social engineering, Zero-day exploits, Cloud computing security threats, and others.

2.4.5. Risk Assessment

Risk is the possibility of something damaging or happening. The Risk Assessment is a process to identify the risks and assess the damage it could cause (Fiona, 2007).

In addition, as stated in VMIA (2010) risk is often characterized by reference to potential events and consequences, or a combination of these. Whereas risk treatment is process of selection and implementation of measures to modify risk (ISO/IEC27001, 2005).

The end result of a risk assessment is justification of any control or safeguards that need to be implemented to mitigate the risk to an acceptable level. The process of selecting controls or countermeasures will complete the Risk Management process (Fiona, 2007).

Appropriate risk management (risk identification, risk assessment, risk treatment), information asset classification, controlling and handling ensure that security is implemented proportionately to and in alignment with business requirements (Office of the Chief Information Officer, 2012).

To prevent threats /problems, it is important to know the risk management approach and act accordingly. In fact, it may not be able to complete prevent these types of problems. However, an approach based on risk management is a useful one. Risk management uses the following approach.

1. Identify risks including their probabilities and impacts
2. Identify possible solutions to these risks
3. Implement the solutions targeting the highest impact, most likely risks.
4. Monitor the risks to learn for future risk assessment

2.4.6. ISM Framework

Perks and Beveridge (2003) consider framework as "…a reasoned, cohesive, adaptable, vendor-independent, domain neutral and scalable conceptual foundation for detailed architecture representation".

On the other hand, as defined in ISO27001-2 (2005) "Framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful". The above definition of framework is used as reference in this paper because it is more comprehensive and suitable for this research work.
Accordingly, ISM Framework is a guideline for developing and implementing ISMS, which is a set of policies and procedures concerned with information security management.

There are several frameworks for IT Governance which relates to information security. However, the most widely used frameworks for information security are: ISO27001, BS7799, PCIDSS, and COBIT (Heru et al., 2011).These ISMS frameworks have different profiles and methodology used in each benchmarks in implementing ISMS for organizations and was discussed in the following section.
Having the concept of information assets, potential threats and risks in the bank industry, the next section discusses the commonly used information security Management frameworks or standards in the world as control mechanism.

2.5. Information Security Management Frameworks

There are a number of choices of information security management frameworks applicable to banking industry. Some of the widely used frameworks are: COBIT, ISO 27001&2, and PCIDSS (Munirul et al., 2011). However, even though these frameworks have been developed and widely practiced in banking sector, each of them has its own strengths and weaknesses. Therefore, customization is relevant to appropriately fit with the bank's environment.

2.5.1. The Three Big ISMS Designing & Implementing Standards

Change of process, change of technology and improvement of user's knowledge about the systems are the main enablers for security threats on information security context. Due to this, lots of standards and compliance requirements are issued by different bodies. The main objective of the standards is to mitigate risks that may arise due to the threats by exploiting vulnerability of the bank (Heru et al., 2011).

As many scholars explained it cannot be denied that nowadays information is a very important asset for any modern organization. Therefore, protecting its security is very important and becoming a top priority for many organizations. Unfortunately there is no single formula that can guarantee 100% of information security. Therefore there is a need for a set of benchmarks or standards to ensure the best security practices are adopted and an adequate level of security is attained.

2.5.1.1. ISO27k Series Standards

International Organization for Standardization (ISO), founded on February 23, 1947, promulgates worldwide proprietary industrial and commercial standards, has headquarters in Geneva, Switzerland (Heru et al., 2011).ISO is "the world's largest developer and publisher of international standards in a wide area of subjects including information security management systems and practices" (Munirul et al., 2011).

ISO as international standardization body is issuing standards in many areas including IT and its security management systems. These standards could either be applied by the member countries (which are around 163 out of 203 countries as Heru et al., (2011) explained) as they are or can be customized to national current development situation and requirements. Implementations of these standards help organizations to effectively manage their information systems security.

ISO27001:2005 Standard

The international standard of ISO/IEC 27001 is one of the ISO standards which specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within an organization (ISO/IEC 27001-2 & Yigezu, 2011). ISO/IEC 2700-2 (2005) standard is derived from the BS 7799:2, 2002, which is meant for Information Security Management System – Requirements and it covers all type of organization (Yigezu, 2011).

Due to the complexity of information technology and the demand for certifications, numerous manuals, standards and national norms for information security have emerged over the past several years. The ISO/IEC 27001 "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification" is the first

international standard for management of information security that also allows certification (BSI-standard 100-1, 2008).

As stated in ISO/IEC 27001-2 (2005) and summarized by Yigezu (2011) this standard contains security recommendations for 12 Security domains which include:

1. Security policy - management direction;
2. Organization of information security - governance of information security;
3. Asset management - inventory and classification of information assets;
4. Human resources security - security aspects of employee joining and leaving organization;
5. Physical and environmental security - protection of computer security;
6. Communications and operations management - management of technical security;
7. Access control - restriction of access control to systems, resources and network facilities;
8. Information systems acquisition, development and maintenance - building security into applications;
9. Information security incident management - anticipating and responding to security breaches;
10. Business continuity management - protecting, maintain and recovering business critical systems, processes and assets;
11. Compliance - ensuring compliance with organizational standards, policies, rules and regulations, procedures and norms; and
12. Risk assessment - analysis, planning, controlling and monitoring of implemented solutions and measures.

ISO/IEC 27001:2005 is always implemented together with ISO/IEC 27002:2005 (Yigezu, 2011).

Figure 2-1. Main contents of ISO/IEC 27002: 2005 adopted from (Yigezu, 2011)

2.5.1.2. Payment Card Industry - Data Security Standard (PCI DSS)

PCIDSS is a worldwide information security standard defined by the Payment Card Industry Security Standards Council (Heru et al., 2011). The standard was created to help industry organizations processes card payments and to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands (Heru et al., 2011). Generally, it is security controls for credit card transactions.

2.5.1.3. COBIT (Control Objectives for Information and related Technology)

COBIT is a certification created by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996 (Heru et al., 2011).

They believe that it is a set of practices (framework) for IT management. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, business risks, and security issues (Heru et al., 2011). It presents an international and generally accepted IT control framework enabling organizations to implement an IT governance structure throughout the enterprise (Yigezu, 2011).

On the other hand, COBIT describes a method for controlling the risks arising from the use of IT to support business-related processes (BSI-standard 100-1, 2008). Further, form currently available standards, only COBIT addresses the full spectrum of IT governance duties (Jimmy, 2012).
COBIT 4.1 has 34 high-level processes, covering 318 control objectives, categorized in four domains:

1. Planning and Organization
2. Acquisition and Implementation
3. Delivery and Support
4. Monitoring and Evaluation

COBIT Version 5 is the current version of COBIT and the complete package consists of: Executive Summary, Governance and Control Framework, Control Objectives, Management Guidelines, Implementation Guide, IT Assurance Guide (ISACA ,1996).

2.5.1.4. Comparison made based on 11 benchmarks

Eleven essential control that should be implemented by an organization, as requirements and compliance of the information security criteria by the standard body of ISMS (Heru et al.,

2011). These Eleven essential controls are applied as basis of parameters and benchmarks to identify the most comprehensively cover all aspects of standard. The eleven controls are:

Information Security Policy, Communications and Operations Management, access Control, Information System Acquisition, Development and Maintenance, Organization of Information Security, Asset Management, Information Security Incident Management, Business Continuity Management, Human Resources Security, Physical and Environmental Security, and Compliance.

All the three standards such as; ISO27001, PCIDSS, and COBIT fulfill the above bench marks as depicted in Heru et al., (2011) than other standards. Thus, ISO, PCIDSS, COBIT become more consideration as best choice.

2.5.1.5. Comparison of The Big Three Standards –based on their profile

Profile of each standard is presented here to provide a general overview and summary of the relevant standard on their respective positions which is currently most widely used worldwide.

	ISO 27001	**PCIDSS**	**COBIT**
Profile of Standards	ISO is a nongovernmental Organization that forms abridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government; also other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations	is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help industry organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise	is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout Organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT
Initiated by	delegates from 25 countries	VisaCard, MasterCard, American Express, Discover Information and Compliance, and the JCBData Security Program	Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)–USA
Launched on	February 23, 1947	15 December 2004	1996
Standards & Components	18,500 International Standards	6 main components on standard	8 main components + 5 components version 3

Certificate Name	Certificate of ISO 27000 Series	Certificate of PCI-DSS Compliance	Certified Information Systems Auditor™ (CISA®) Certified Information Security Manager® (CISM®) Certified in the Governance of Enterprise IT® (CGEIT®) Certified in Risk and Information Systems Control TM (CRISCTM
Scope Information Security	Scope Information Security	Information and Data Transaction Security on debit, credit, prepaid, e-purse, ATM, and POS	IT Governance
Usability	163 national members out of the 203 total countries in the world	125 countries out of the 203 total countries in this world	160 countries

Table 2.2. Profile of Big Three of ISMS Standards; Adopted from (Heru et al., 2011)

Nowadays, it is very important for a standard, accepted and recognized as global benchmarking tools ISO's most widely used in globally by163 countries, compared with PCIDSS (125), and COBIT(160). Indication depict that ISO is more easily implemented, stakeholders (clients, suppliers, customers and management) is easier to recognize, also it has appropriate platform in an organization deal with, than two others security standards *(*Heru et al., 2011).

Conclusion remarks

Each standard playing its own role and position in implementing ISMS, several standards such as ISO/IEC 27001 focusing on information security management system as main domain, while PCIDSS focus on information security relating to business transactions and smartcard, then COBIT focuses on information security and its relation with the Project management and IT Governance *(*Heru et al., 2011). In addition, COBIT typically covers a broader area while ISO/IEC 27001 is deeply focused in the area of security, (ISACA, 1996). Thus, the scope is narrowed for the two standards such as ISO 27001 and PCIDSS both focused on information security. But which comes first?

2.5.1.6. Which must come first, ISO27k or PCI DSS?

As we can see above PCIDSS and 27001:2/2005 (ISO 27k) are focused on Information Security. If you are financial industry stakeholder, for sure both are required by you and you

may or may not be puzzled with the same question stated on the Title, which I should work first?, ISO27K or PCI DSS? (Endale & Gary, 2012).

The simplest and theoretically exact answer for this question is either of them. However the right answer differs from organization to organization. Therefore, it is better to mention the different options which are stated by (Endale & Gary, 2012).

- **Option 0.** Do nothing.
  *A**dvantage:** none!*
  ***Disadvantage**: Compliance failures & penalties. Other information security incidents & costs could happen at any time. On top of all, this option misses opportunity for improvement.*

- **Option 1.** *'Do' PCI-DSS only. Get it done without regard to the bigger picture.*
  ***Advantage**: relatively small, focused project should be effective, quick and low cost. Management is at least thinking about security and risk and compliance, albeit myopically!*
  ***Disadvantage**: it will not address all the other information security and information risk management requirements that extend way beyond PCI DSS. This is a tactical approach, not strategic. Also the PCI DSS solution may be suboptimal in the long run (for example constraining the way you set up network, system and application security).*

- ***Option 2.** 'Do' PCI-DSS as introduction to a bigger compliance project.*
  ***Advantage:** It should be seen as part of a bigger whole. Gives the organization a chance to figure out, design, develop and get to use and manage decent PROCESSES that should have wider, long-term value. Puts things in place for the ultimate solution, at not much more cost/time than option 1.*
  ***Disadvantage**: Still only PCI-DSS focused. Still compliance focused. May be such a troublesome project that it puts management off doing anything else unless they have to!*
- ***Option 3.** 'Do' ISO27k, but prioritizing PCI-DSS compliance to generate an 'early win'.*
  ***Advantage** : The more comprehensive ISO27k approach will bring numerous benefits – for instance the management system elements will help management to appreciate and fulfill their wider obligations towards protecting/securing information, gaining/maintaining trust, addressing risks before they materialize and afterwards, and so forth. The 'early win' part, if handled and promoted well, should help sell the benefits to management and other stakeholders, and position the ISMS in a positive light.*
  ***Disadvantage**: Management needs to be made aware of the costs and benefits of ISO27k, since it usually implies a substantial investment and extensive changes.*

As Endale and Gary (2012) recommended, in general terms it is known that business interest is a foundation for business activity, but compliance comes in order to assure the continuity of the activity. That means compliance is a subset of business interest. From the above analysis, one can learn that ISO27k is focused on fulfilling security requirements of a business interest, that may or may not include PCI DSS, and PCI DSS is focused on business activity compliance.

2.5.2. The More Appropriate Standards for Banking Sectors

Since both PCIDSS and 27001:2/2005 (ISO 27k) are focused on Information Security and applicable for financial institutes, it is possible to use either of them. However, PCIDSS is applicable for small project and it does not see security of a Bank as a whole whereas 27001-2:2005 help to design and implement a compressive information security in a Bank.

ISO27k series specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the Bank's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual Banks (Mohan & ISO2k Implementers' forum, 2012).

Therefore, 27001-2:2005 help to design and implement a compressive information security in a Bank than PCIDSS.

2.5.3. Information Security Management and its Organizational Structure

The structure of IT department has a great contribution or impact in information security management. The generalist approach is prone to attack, employees' dissatisfaction, as a result turnover will increase.

Most banks have separate streams or verticals to manage their IT in some form or the other, such as technology solutions, infrastructure management, systems management and IT information security, among others. The primary responsibility of these groups is to manage their individual areas in terms of delivery, ensure compliance to the IT policies of the bank and drive the innovation or business programs that the IT committee of the bank proposes. IDRBT (2011) recognizes that there is no unique security organizational structure.

2.5.4. ICT Profile and Standards in Ethiopia

Computers were introduced in Ethiopia back in 1960's when the first IBM computer become functional (Yigezu, 2011).

The growth of IT sector in the Ethiopia has been limited because of different factors: low level of literacy, price for IT equipment, lack of infrastructural development, lack of trained

man power, etc. However, despite all these constraints, the development can be seen in building ICT supported networks like the SchoolNet, WoredaNet, UniversityNet, AgriNet, and HealthNet though it is still the least developed (Tomonari, 2008).

Even though e-government is at its emphatic stage in Ethiopia, there are different projects already implemented and some are underway. Among the already implemented projects are the WoredaNet, which interconnects more than 600 woredas all over the country (Tomonari T., 2008). The services that are offered by this network are videoconferencing services, directory, and internet services.

Even though, Ethiopia shows a good growth in ICT infrastructure, however, from the information security standardization aspect there is no nationwide framework which is applicable in Ethiopia. As Federal Democratic Republic of Ethiopia (FDRE, 2011) stated that the value and importance of information and information infrastructures has become conceived at national level. And it is difficult to ensure peace, democratization and development without it. Thus, to protect information FDRE has published National Information Security policy even though it is focused mainly to compliant external standards.

Further, there are indications that show organizations in Ethiopia at different level of understanding and acting with regards to requirements, security risks, auditing and various threats mitigations (Yigezu, 2011).

As shown under section 2.5.1.5 above the most widely used international standard for information security management – sometimes called ISO27k series, is requirements oriented, meaning that it states the requirements organizations should satisfy if they want to undergo certification in accordance with the standard (Fredrik, 2005). However, the standard does not mention how this can be attained. On other words, how Banks in Ethiopia identify their requirements prior to select best practices or controls? Does the standard clearly show the steps or methods that any organization can follow in their requirement identification process when they develop ISMS? The proposed ISM Framework addressed this question.

Due to this challenge banks may outsource information security management system development and implementation process because they don't have in-house capability to perform this vital task. They hire experts to develop and implement ISMS, and the resulting ISMS is only as good as the experts who perform it. Often, the consumers of such services have no way to understand if the ISMS developed for them is adequate for their enterprise (Fredrik, 2005).

2.5.5. Methodologies used in Developing ISM Framework

Different research approaches are made to develop security related framework by information security domain scholars. For example, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and ISO27k series are employing an open brainstorming approach for gathering and analyzing information in addition to standard consumers' comment, and through conducting rigorous research to develop ISM Framework (Fredrik, 2005).

Others scholars conducted Information Security Auditing Framework research using mixed research method (Qualitative and Quantitative) as a research paradigm (Yigezu, 2011).

2.6. Research Design Approach and Steps used for ISM Framework Development

There is no a unique conceptual ISM Framework development research process among scholars. As a result different scholars' ISM Framework development research process will be governed by the following main research design components and steps as shown below (Are, 2007).

2.6.1. Main Research Design Approach

Some scholars design their research in the following order: literature review ➔ Case study or Assessing ➔Propose a conceptual ISM Framework (Are, 2007).

Others follow: literature review ➔ Propose ISM Framework ➔ reviewed by professionals and tested in the real banking environment (Munirul et al., 2011).

To elaborate these points in their order:

1. Conduct a review of literature in banking information security management, that includes an in depth review of literature in information security management viewpoint, and perform a comprehensive analysis of literature on information security management.
2. Developed a conceptual model of a solution to the information security management problem stated in the research proposal.
3. Demonstrate the conceptual model of the solution to the research problem by the following ways:
    a. Conducted in-depth structured interviews of senior executives, with decision-making responsibilities for security management in their organizations, using a set of interview questions that were derived from the draft conceptual model.
    b. Presented summary of a draft conceptual model, at national and international professional and academic conferences, for review by group of peers, academics, security management professionals, managers, and senior executives from various industries.
    c. Outline how the conceptual model of the solution could be implemented in an organization (Anene & Annette , 2007).

One single design cannot serve the purpose of all type of research problem .It also varies because of the following points: The means of obtaining information, availability and skill of the researcher, the objective of the problem to be studied, the nature of the problem to be studied, availability of time and money for the research work (Kothari, 2007).

2.6.2. Steps that are undertaken in ISM Framework Development

The steps which are undertaken in ISM Framework research by different researchers may not the same (Anene & Annette, 2007). However, as stated by (Anene, 2007) they share the following steps/ methods of investigation in some order adjustment:

1. Reviewed literature in ISM viewpoint
2. Conduct in depth interviews with security management decisions
3. Developed a conceptual model of the solution to the research problem
4. Presented summery of conceptual solution at national and international professionals and academic conferences for peer and practitioner reviews
5. Demonstrated the conceptual model by outlining how the conceptual solution could be implemented in an organization

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

This chapter presents what research design and method was employed to answer the research questions formulated. Review of the research methods: qualitative, quantitative and mixed research methods are made and choice of the research methods and the reasons for that is stated. Questions answered in this part are: What research paradigm is used? How samples for the study are selected and why? What data collection techniques are employed? How data is analyzed?

3.1 Main Research Design Components and Steps used for ISM Framework Development

A conceptual ISM Framework development process has followed the following main research design components and steps which guide the research process. research design is a blue print or guidance of the research (Kothari, 2007).

3.1.1 Main Research Design Components

The student researcher preferred the following research design to reach a sound and applicable ISMF. On other words, to answer the research question properly.

a. ***Literature Review:*** This research starts with a literature review focusing on key concepts from the areas of information security management studies.
b. ***Assessing The Current ISM Practice and Challenges:*** A mixed research methods (Qualitative and Quantitative methods) was applied to assess the current ISM practice, success factors, and problems that impede the implementation of ISMS in the banking sector .The rationale for selecting mixed methods design is to get a better understanding of the problem identified in this research. The mixed methods approach would allow for both text and statistical analyses of data, and would permit more flexibility when designing questions for survey interviews, i.e. both open- and close-ended questions (Anene & Annette, 2007).
c. ***Propose a Conceptual ISM Framework:*** The conceptual ISM Framework was modeled based on literature review findings and the assessment result of the current ISM practice.
d. ***Evaluating the proposed ISM Framework:*** The proposed conceptual ISM Framework was evaluated by professionals (domain experts) and refined based on the sound comments and suggestions.

The overall thesis structure is governed by the following main research design components and steps as shown below:

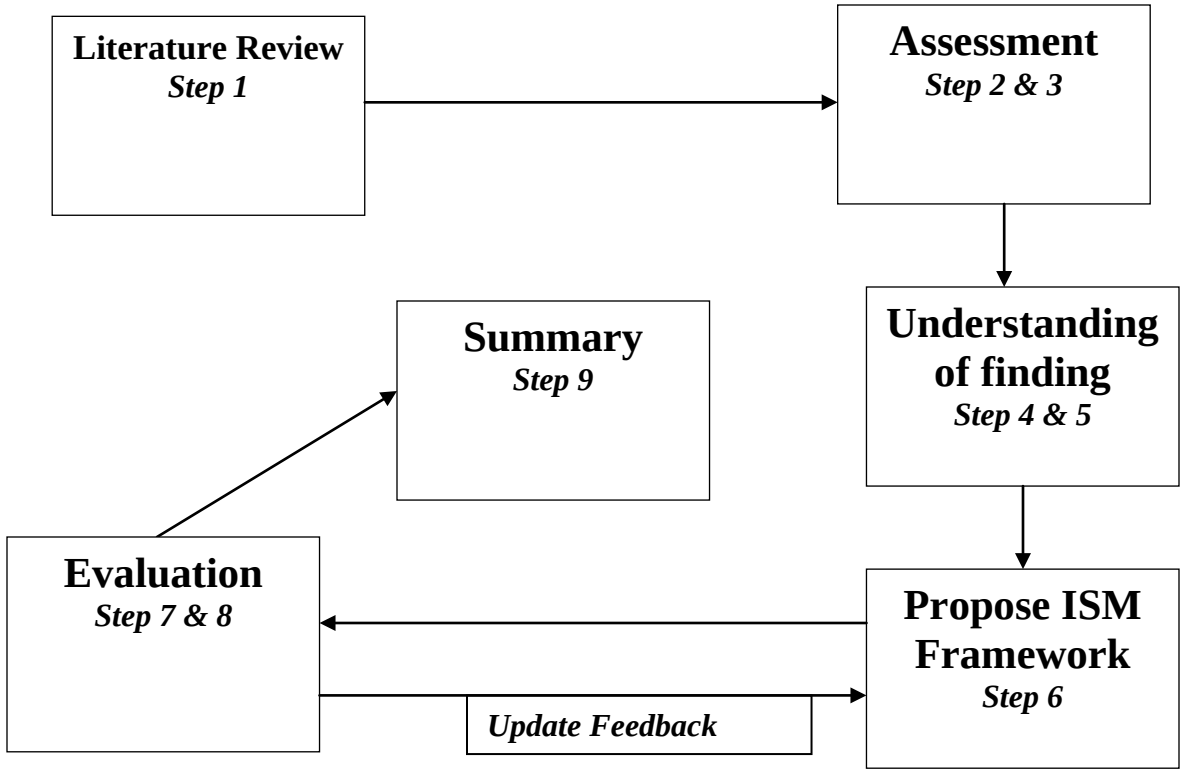


Figure 3-1. Depicts the research design and steps

3.1.2 Steps that has been taken during this study

1. Conducting a literature review to capture ISM concepts
2. Assessing the current ISM practice and challenges
3. Collected data was analyzed
4. The findings resulting the data analysis (3) will be discussed with respect to the research question
5. These findings (4) were interpreted within the context of the research framework.
6. A conceptual ISM Framework was proposed based on the findings of the literature review and assessment result
7. Evaluate the conceptual ISM Framework by domain experts
8. Incorporate the sound feedback to a conceptual ISM Framework
9. The thesis concludes with a summary of the findings and final ISM Framework

3.2 Research Methodology

The research design was impacted by the result of the literature review. The study was conducted using survey questionnaire, document analysis, and interview as a method of data collection and mixed research method as a research paradigm. The strategy of inquiry for this

approach is concurrent procedures. Concurrent procedures strategy is defined as situations "… in which the researcher converges quantitative and qualitative data in order to provide a comprehensive analysis of the research problem" (Anene & Annette, 2007).

Mixed methods research refers to the research or lines of inquiry that integrate one or more qualitative and quantitative techniques for data collection and analysis. Qualitative collection methods, including interviews, focus groups, participant observation, and open-ended survey items have great potential for exploring new topics, assisting theory building, and providing context for quantitative data (Matthias et al. ,2012). Open-ended questions are used in organizational research to explore, explain, or reconfirm existing ideas. Whereas quantitative methods work best in isolating variables and demonstrating correlates associated with variation, qualitative data collection techniques are particularly effective at gaining insight into the processes and events that lead up to the observed variation (Dean et al., 2008).

Combining, or linking, quantitative and qualitative data collection methods within studies can provide numerous benefits. These advantages are described for three broad reasons:

- To enable confirmation or corroboration of each other via triangulation;
- To elaborate or develop analysis, providing richer detail; and
- To initiate new lines of thinking through attention to surprises or paradoxes, providing fresh insight (Dean et al., 2008).

Mixed methods research is defined as a technique that "mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study" (Dean et al.,2008). Mixed methodology today is a natural complement to traditional qualitative and quantitative research.

Therefore, to conduct this research the student researcher used descriptive survey method. This method was selected for this particular study because it was found an appropriate technique for collecting vast information and opinion from respondents. It is also relevant to gather detail description of existing condition and practices of Information Security Management in the bank industry.

3.3 Source of Data

The primary data sources used in this study are eIT managers who have decision power related to IT security. This is because, IT departments manage all the information systems functionalities including its security while the security experts or system administrators make sure that the systems are functioning as per the required policy, procedures, bank's requirement, etc.

In addition, secondary sources of data such as relevant best practices in information security policy, standard and procedure documents were reviewed.

3.3.1 Sampling Design and Sampling Techniques

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

3.3.2 Population

The population of the study was twenty (20) private and government banks (Head quarter) in Addis Ababa. Among those, five banks were selected. And the researcher collected 5 (five) banks' data.

3.3.3 Sampling Method

This study employed both Non-probability and probability sampling method. The researcher used the lottery sampling technique; as such it is a Non-probability sample method, for interview and questionnaires purpose in all sample public and private banks. Because of the time constraint the sampling method used for the interview was purposive sampling technique and as such, it is a non-probability sampling. Purposive sampling refers to situations where participants are selected based on their specialized insight or special perspective, experience, characteristic, or condition when there is something the researcher wishes to get and understand (Yegidis & Weinbach, 1996) .

In addition, probability sampling was used to select sample banks out of twenty banks. To select sample banks additional techniques were used. That is, stratified sampling to differentiate the public and private banks and lottery method to select sample banks from each strata.

From the total number of twenty private and government Banks found in Addis Ababa city Administration five banks were selected for the study.

The following procedures were generally used in determining the sample:

1. The total number of Banks, by name, has been taken from National Bank of Ethiopia (NBE).
2. Then apply stratified probability to differentiate the public and private banks since they are homogenous.
3. The proportion for selection was determined by computing the ratio of the required sample (n) to the population of the study (N), proportion 5/20=1/4.
4. The stratified bank was multiplied by the obtained proportion to get the number of banks that are included in the sample of the study.
5. Apply lottery method to select sample banks after stratified sampling was done.

6. Purposive sampling technique was applied to IT security managers of sampled banks.
7. Distribute questioners and conduct interview with IT managers in the five sampled banks.

3.3.4 Sample Scope

Sampling scope refers to a list or set of direction that identifies the target population. Thus, the target population of this study is those 5 (five) selected Banks.

3.3.5 Sample Size

The sample size of this study is 5 banks. This means 25% of the total population ((5/20)*100%).

3.4 Instruments of Data Collection

Generally, three types of instruments, namely: questionnaire, Document analysis and interview were employed for the data collection. The primary data was collected through questionnaire (structured) and interview (unstructured).

3.4.1 Questionnaire

A questionnaire was designed based on the three categories such as Physical and Environmental, Technical, and Administrative. The questions items are open and closed on practices and status in Information Security Management process. The questioners were prepared and distributed to IT manager of the respective sampled Banks.

The questionnaire developed for IT manager had 55 questions in three categories. The first section dealt with physical and environmental security management of the respondent bank. The second section inquired about the technical aspect of information security. And the third section deals with the administrative aspect of information security.

3.4.2 Interview

Informal information about interviewees' experience and knowledge has been collected by the researcher prior to conduct an interview. They possess the experience and perspective in information security management that this research wishes to understand. Given the security management experience and background of potential interviewees, purposive sampling method seems the most logical choice for data collection in this research (Anene & Annette, 2007).

The main purpose of this interview session is to supplement and increase the validity and reliability of the information obtained through the questionnaire. The following points were addressed. These are: *questions about ISMS development and implementation practice, what are the problems that impede and the success factors in development and implementation of ISM System and how do you identify your bank's requirements prior to select best practices or controls?, and what kind of IT risk management methodology used?*

The appointment was given to interviewees approximately three days before their scheduled interview date. The average time for the interviews was 50 minutes. All interviews were conducted face-to-face, in person, at the interviewees' site of business.

3.4.3 Document Analysis

Document analysis has been made as believed necessary. Printed materials; books, journal articles, conference proceedings, and internet sources were used to know the subject area in depth, and assess other countries experiences in fighting against their Information systems security threats. Moreover, one bank's information security policy and procedures has been reviewed.

3.5 Pilot Study

In order to assess the relevance of the instruments designed to collect data for the study, the pilot study was conducted in one of the sample Banks. The aim was to find out and avoid ambiguity, omissions and misunderstanding of each item. Using the relevant comments from results of the pilot study and suggestions of the advisor corrections was made. Some of the changes that have been made are: The multiple choice questions and a rating scale questions were changed to the dichotomous question answer type. Further the number of questions reduced to 55. Moreover, correcting some vague questions was made.

3.6 Procedures

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. Finally, the student researcher was proposed ISM framework.

3.7 Method of Data Analysis

After the collecting of 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 charts, and verbal descriptions was used to present the data.

CHAPTER FOUR

FINDINGS INTERPRETATION AND IMPLICATION

The findings are organized in to three basic categories namely, Administrative, Technical, and physical & Environmental security. Each category has list of security domains. In this section findings of the study and its interpretations are presented under each question items whereas implications are stated at the end of each security category.

4.1. General Information

The aim of the field study is to discover the state of the information system security management of banks involved in financial services to the people using IT. Questionnaires and interview questions were used as instrument to carry out the study. The questionnaires were used to collect data about security domains defined by ISO 27002 and the student researcher own additional points which are relevant to inspect ISM practice in the banking industry. The summary of the findings of each question item under each security domains in the surveyed banks is attached at the end as ***appendix D*** in which the banks are namelessly represented from 1-5.

The thesis research findings are classified into two major areas viz.; findings from the interviews and findings from questionnaires. Questionnaire findings provided insight into how information security is managed in surveyed banks. Findings from Interview clarified the general issues in information security management in addition to supplement the questionnaires.

4.2. Study Sample

The following banks were included in the study. These are: Commercial Bank of Ethiopia (CBE), Construction and Business Bank S.C. (CBB), United Bank S.C. (UB), Oromia International Bank S.C. (OIB), and Nib International Bank S.C. (NIB). These banks were selected by lottery method.

4.3. Respondent Information

The respondents of the research include IT staffs who are engaged in managerial position and decision maker about IT security. The job title of these officials are manager IT security, Deputy IT manager, and IS process owner.

4.4. Problems

The problem that the researcher faced during the survey was getting senior IT managers since CORE banking implementation makes them so busy. The other problem was to get feedback on intended dates and time because of respondents' busyness and getting bored with such

survey questions. There were cases where three to four visits and many phone calls were made to get responses. This could be considered as a major problem that significantly slowed down the research.

4.5. Questionnaire

The questionnaire was given to IT staffs in one of the sampled bank as a means of testing whether the questions were easily understood. After accommodating recommendations from these groups of people and my adviser, the questionnaires were personally distributed to the banks listed in 4.2. And then the student researcher has collected the filled questionnaires. The questionnaires are attached as an ***appendix A*** at the end of this document.

Cooperation letter which was written by Addis Ababa University and introductory statement about privacy of respondents is a document which is attached to a survey questionnaire in order to raise the motivation of the respondents and to create comfort zone. This is used as a guarantee that the information provided is to be used only for the stated purpose.

The survey was carried out in 5 Ethiopian banks from April 05 - 25, 2013. The survey was done in person to increase the response rate and also succeed in the study even though it is time taking to get responses from a given bank.

4.6. Response

Questionnaires were collected from all the 5 banks to which questionnaire were distributed. Therefore, the response rate is 100% calculated using:

$$\frac{\textit{Number of completed questionnaire}}{\textit{Number of questionnaire sent out}} = \frac{5}{5} = 1.0 \times 100 = 100\%$$

This shows that the response rate is high and it could be considered valid for proceeding with the analysis of data obtained.

4.7. Findings

In this section, the results from data analysis are presented and addressing the main components of information security management which make up the themes .The data analysis result is depicted using charts in percentage which refers to the number of banks having or not having certain security situations. As has been indicated in 4.2 (response) above, the result of the analysis is based on the responses obtained from 5 banks. For the sake of simplicity findings of the questionnaire was summarized and attached as an ***appendix C*** at the end of this document.

All control domains are categorized in to three based on the idea of Anene et al., (2007). The focus of information security evolved from physical security of computer centers to technical and then administrative security.

4.7.1. Physical and Environmental Security

Banks were asked whether they have physical and environmental security and the result is summarized as shown in figure 4-1 below.

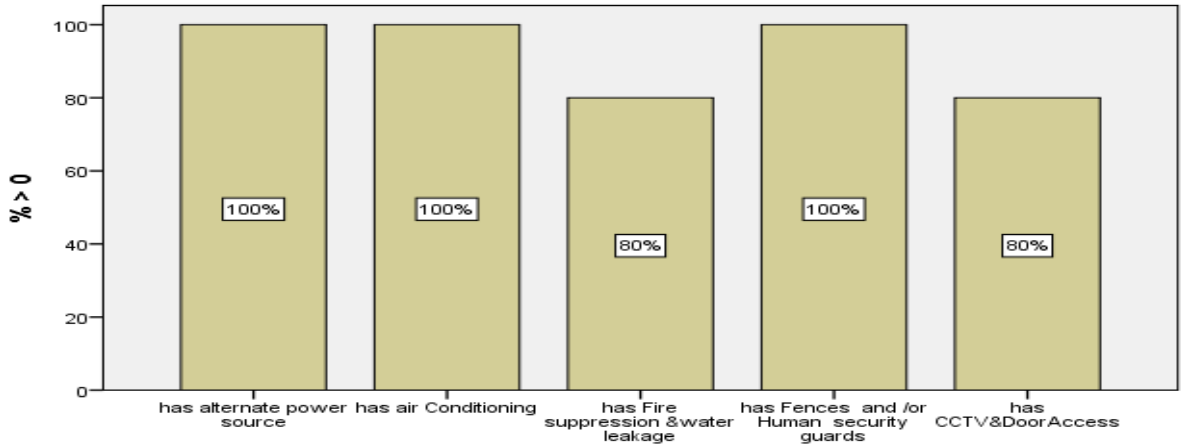


Figure 4-1 alternate power, AC, Fire extinguisher system, fences, and CCTV camera & door access system

As shown in figure 4-1, the finding from the survey shows that 20% of the banks surveyed don't have fire suppression, water leakage, door access control, and CCTV system while the rest 80% possesses. But when it comes to alternate power supply (generator), Air Conditioning, fence and security guard all surveyed banks have employed.

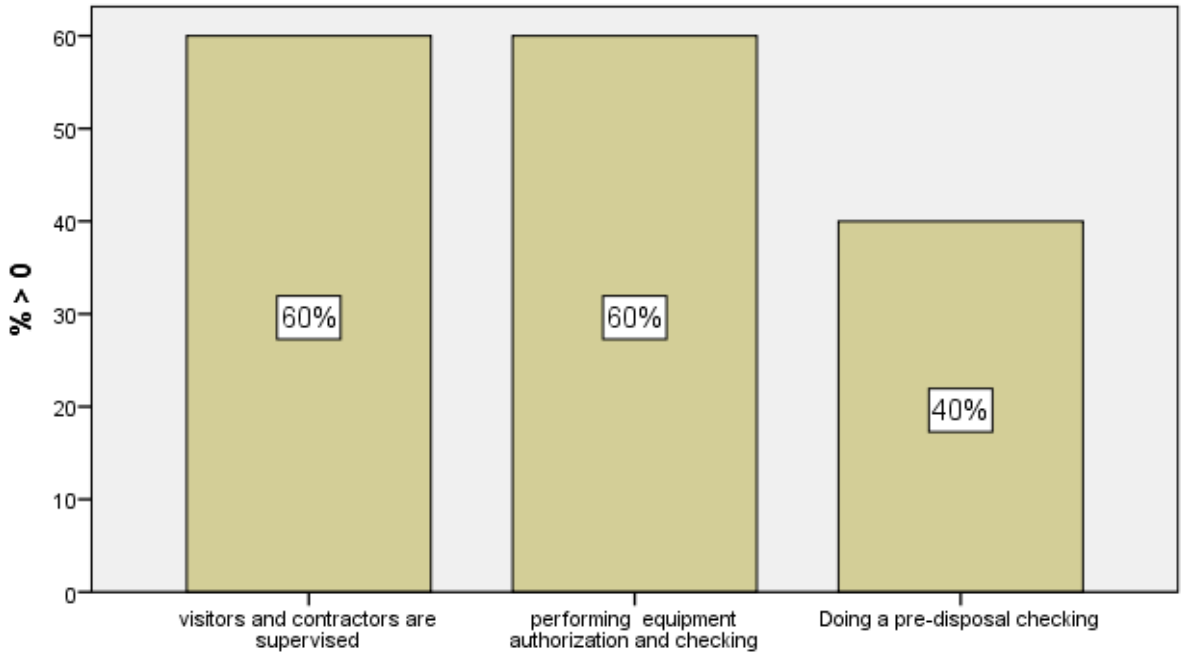


Figure 4-2 visitors & contractor's supervision, equipment pre-disposal authorization and checking.

As shown in figure 4-2 above, 40% of the banks surveyed do not supervise the visitors and contractors when they visiting the data center /server room while the rest 60% supervises them.

In 60% of the surveyed banks, authorization and checking occur on equipment entering or leaving your site while 40% did not do same. Moreover, in 40% of the banks, sensitive data and licensed software removed from data-storage equipment prior to disposal but 60% of the banks did not do same.

Implication

Most surveyed banks in general, have enough physical and environmental security facilities for their sensitive and mission critical equipment like servers, even though they are weak in visitor and contractor supervisions.

4.7.2. Technical/Operational Security

-Communication and Operation Management

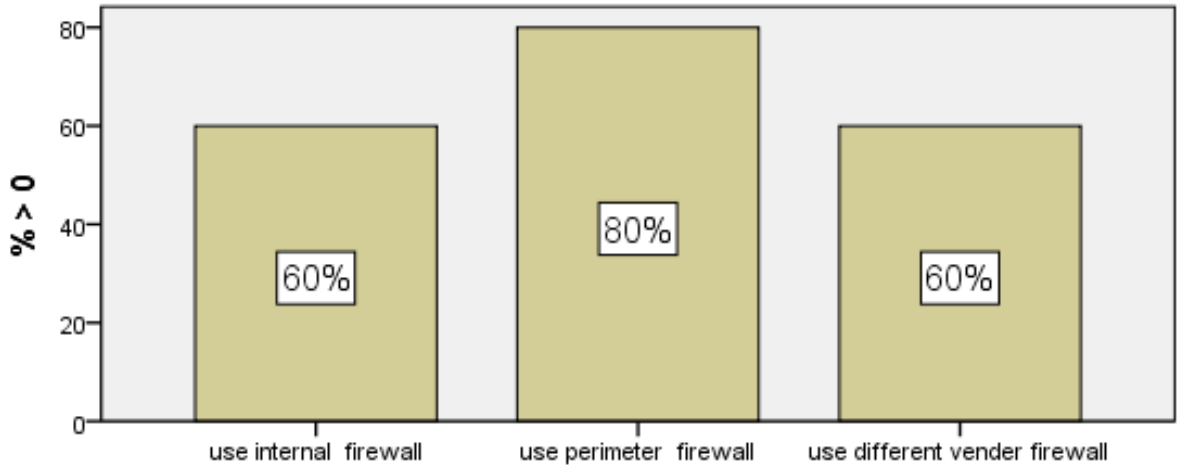


Figure 4-3 Intranet and Internet firewall placement

60% of surveyed banks used an internal firewall which is between intranet and DMZ (demilitarized zone) and 80% of them used an external firewall which is between the DMZ (demilitarized zone) and internet or outside world. In case of vender 60% uses the different vender firewall for the internal and external perimeter firewall.

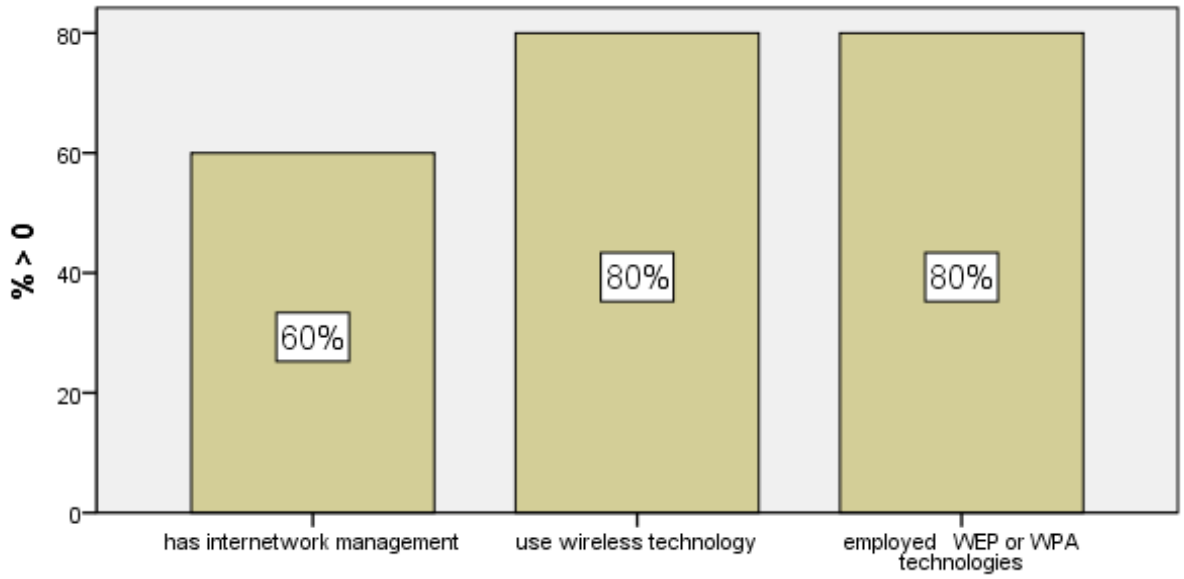


Figure 4-4 internetwork management system, and wireless security

As shown in figure 4-4 above, 60% of the surveyed banks implement internetwork management system like Cisco works or Cisco Access Control server or Cisco Security Management Systems. In case of wireless technology 80% of the surveyed banks have

implemented wireless network and used authentication and encryption technologies like WEP for Wireless LAN network security.

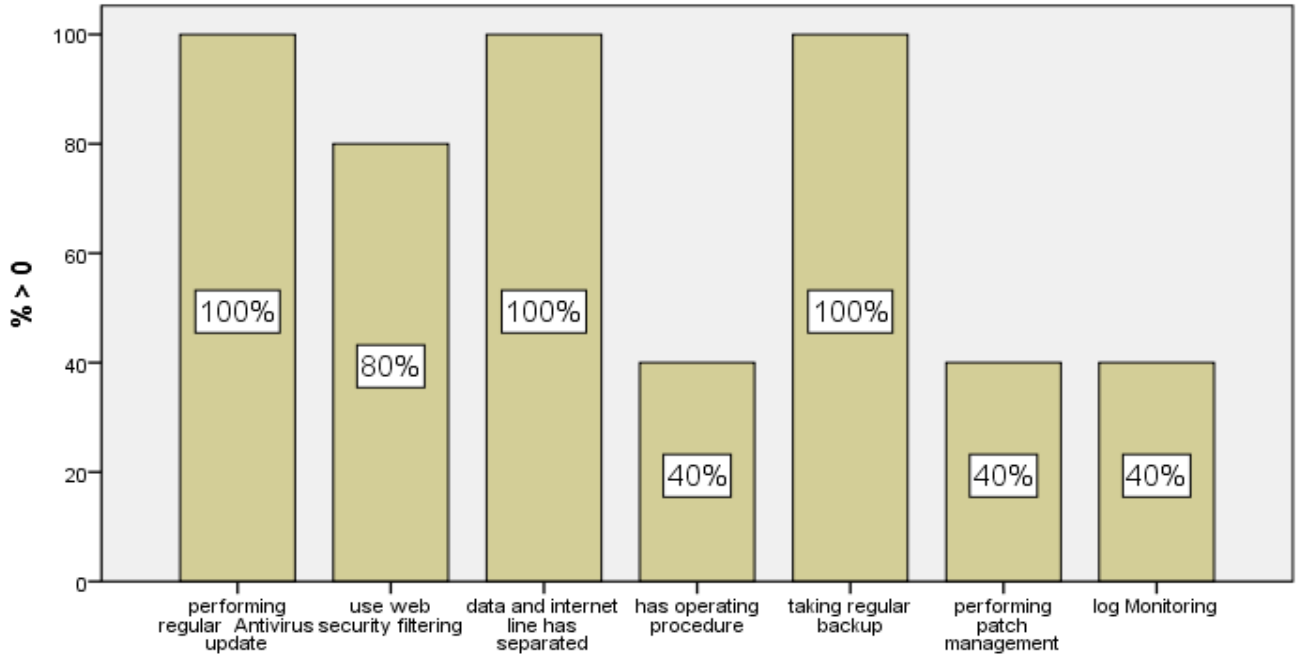


Figure 4-5 antivirus, web traffic filtering, line separation, Operating procedures, taking regular backup, patch management and log monitoring.

100% of the surveyed banks has installed and regularly update antivirus on computers that they possess. In addition to antivirus, 80% of them protect web traffics originating from untrusted network using firewall, Unified threat management System (UTM), and Web filters (IronPort). Moreover, all surveyed banks have separated Internet line and data line (for example CORE banking data) to insure security of their data from malicious attack.

On top of that 40% of the surveyed banks have documented operating procedures such as for back-up, and equipment maintenance and 100% of them takes daily back up of financial data and other like human resource data has taken weekly bases.

40% of surveyed banks have patch management procedure to known vulnerabilities and 40% of them logged and monitored system logs.

-Access control

The majority of banks follow some steps when a new system (such as Firewalls, Routers, and Switches etc.) is installed on the network as shown below, figure 4-6.

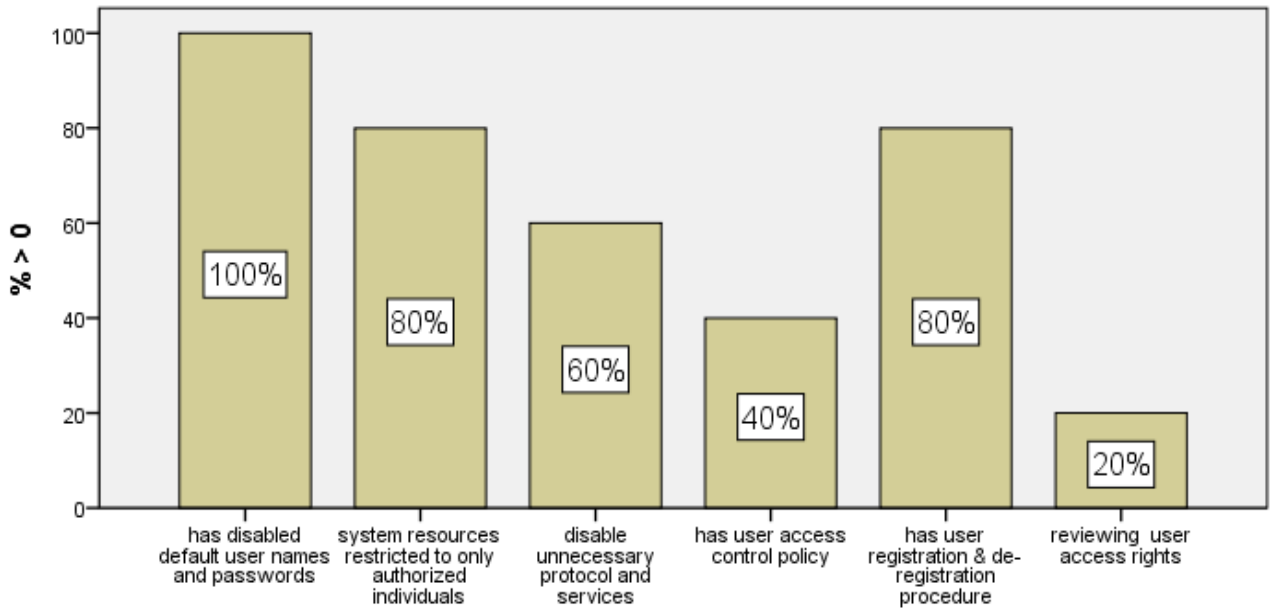


Figure 4-6 disable default user account, restriction, disable protocol, policy for user registration & access control, and reviewing user access rights.

Figure 4-6 shows that 100% of surveyed banks changes default passwords and disable user accounts immediately. In case of access rights to system resources 80% of them restrict any system to only the individuals that are authorized to use those resources, and 60% of surveyed banks close /disable any unnecessary protocol and services.
In addition, 40% of the surveyed banks have access control policy documents for granting access to information systems. And 80% of them has formal user registration and deregistration procedures to manage users who have access to information systems.

Only 20% of the surveyed banks have procedures to review access rights they grant to users as required.

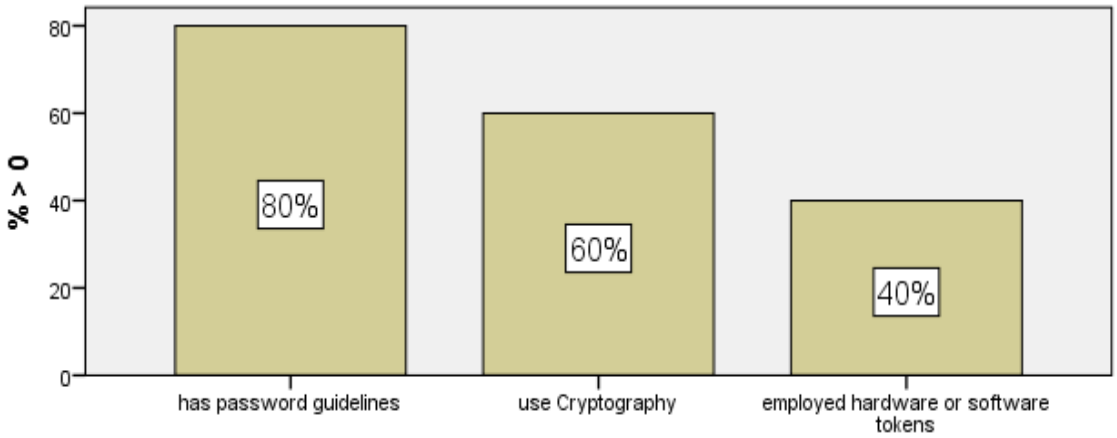


Figure 4-7 password guidelines, and authentication mechanisms

As shown in figure 4-7 above, 80% of the surveyed banks have password usage guidelines (about its complexity, change period, password reset, access attempt and lockout) for the users to select and maintain the security of their passwords.

Those banks use additional authentication mechanisms to ensure the security of their information systems. For example, 60% of the surveyed banks use cryptographic (Encryption & Digital signature) based technique while 40% of banks use hardware tokens.

-***System development***

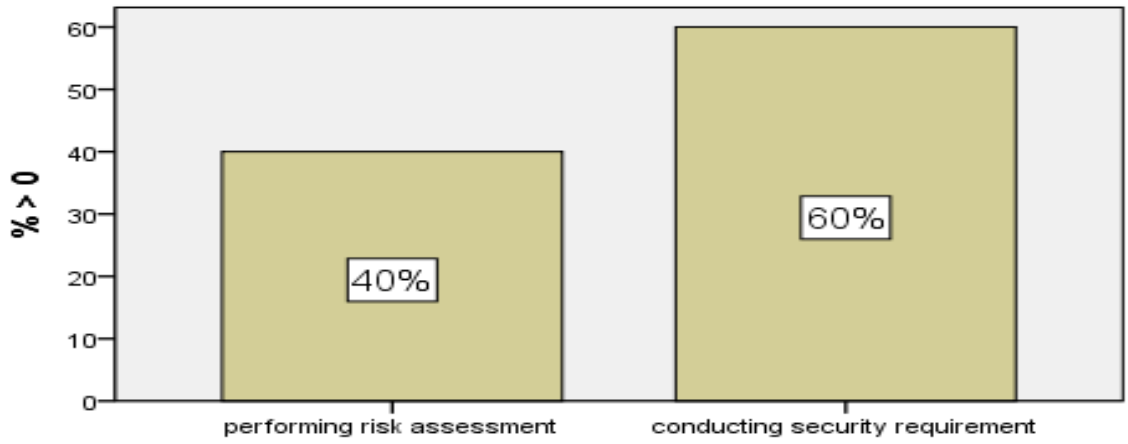


Figure 4-8 security requirements identification in system development process

In this category, as shown in figure 4-8 above, 40% of the surveyed banks execute business risk assessment to identify security requirements prior their system development process. And 60% of those banks conduct system security testing before production.

Implication

In general speaking, surveyed banks have medium technical security facilities to protect their sensitive and mission critical information even though they are so weak in patch management, system log monitoring, performing risk assessment, user access control and reviewing their rights.

4.7.3. Administrative /Organizational

-***Security Policy***

The sampled banks were asked whether they have security policies & procedures, its implementation status, update frequency, and standards they used. The result is summarized as shown in figure 4-9, 10, 11, and 12 respectively as shown below.

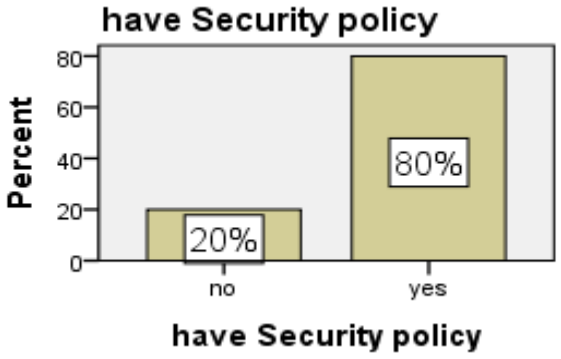


Figure 4-9 Security policies and standards

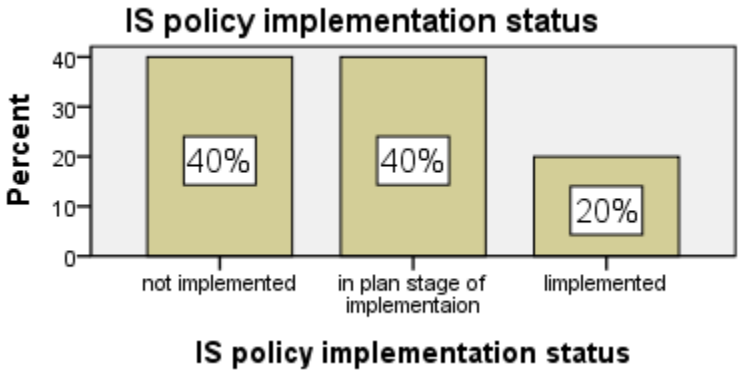


Figure 4-10 policies implementation status

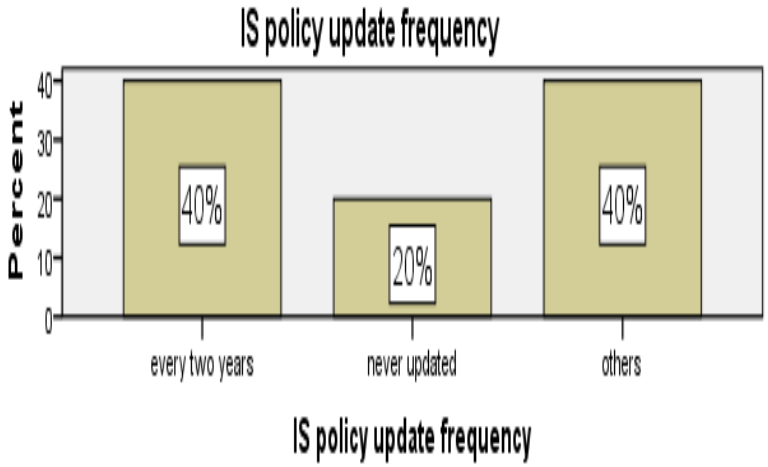


Figure 4-11 Security policy update frequency

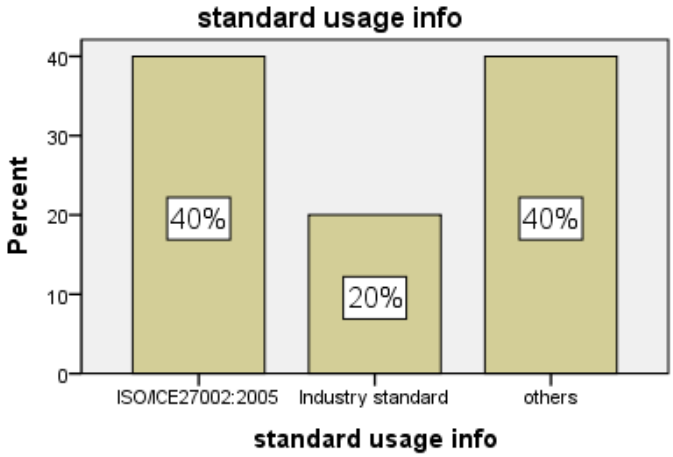


Figure 4-12 standards usage information

As shown in figure 4-9 above, the findings from the survey shows that 20% of the banks surveyed don't have security policy document while the rest 80% possesses the document which they cascaded and adopted from the national and international information security policy.

As depicted figure 4-12 above, 40% of the surveyed banks use ISO/IEC 27002:2005, others 20% use Industry Standards and 40% of those banks use other standards like in house developed. But when it comes to implementation, as shown figure 4-10 above, only 20% of the banks have implemented their security policy and 40% of surveyed banks that have the policy document are in plan stage of implementation. The rest 40% are undertaking the preparation and are planning to create the document and will implement it soon.

As shown in figure 4-11 above, 20% of the surveyed banks have never updated the security policy. This is mainly due to none of them being fully implemented so far. 40% of those banks have updated every two years and other 40% of banks updated as required, there is no pre-defined plan for updating.

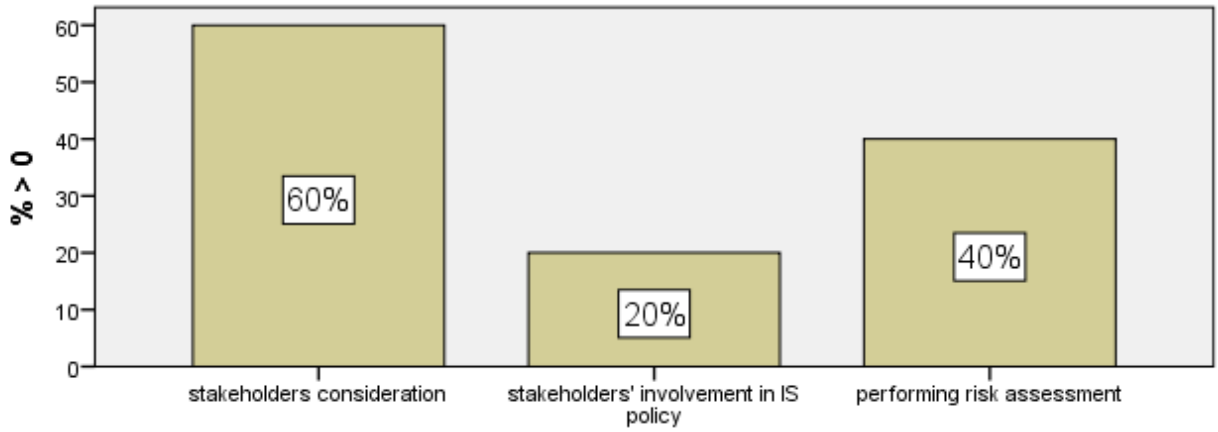


Figure 4-13 Stakeholders consideration, involvement, and risk assessment

As shown in figure 4-13 above, 60% of the surveyed banks have considered stakeholders (such as employees, contractors, suppliers/venders, service providers, and customers who have access to the bank's network) in their information security policy development.

In addition, 20% of those banks have allowed (to participate) the stakeholders such as Security specialists, technical staff, administrator (or HR), legal advisor, internal Auditor, Risk and compliance, and Top management in the designing and implementing process of information security policy.

Only 40% of surveyed banks are performing risk assessment to identify security requirements prior to select best practices or controls whereas, 60% of banks did not perform risk assessment.

-Organizational security

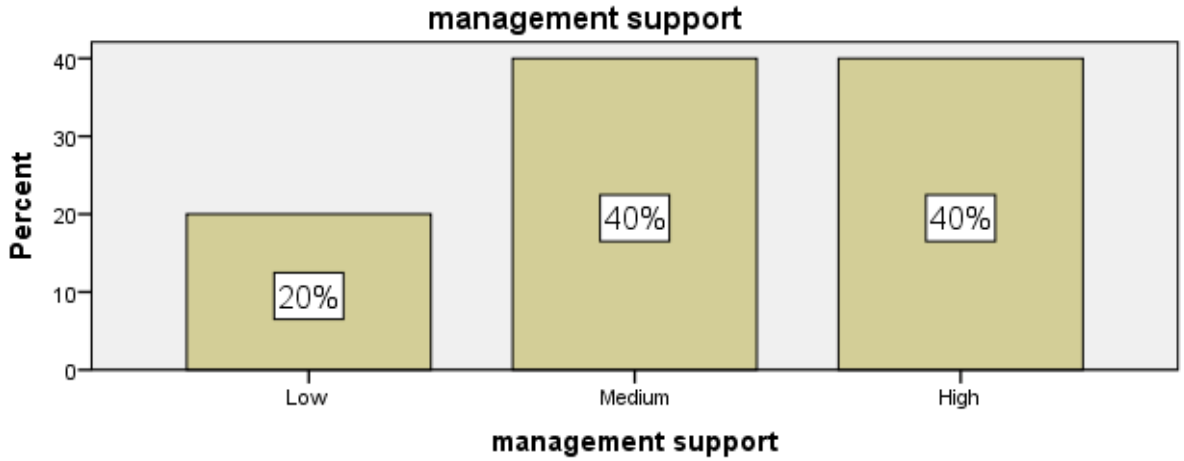


Figure 4-14 Management support

As depicted in figure 4-14 above, in Information System security assurance process, surveyed banks has low, medium and high management support with 20% , 40% and 40% respectively.

As shown in figure 4-15 bellow, 100% of the surveyed banks have faced a problem of: lack of experienced security staff on international standards, lack of local Information Security Management Framework/standard, and annual budget for information security. As a result, these problems are hindered the implementation of ISMS in their bank.

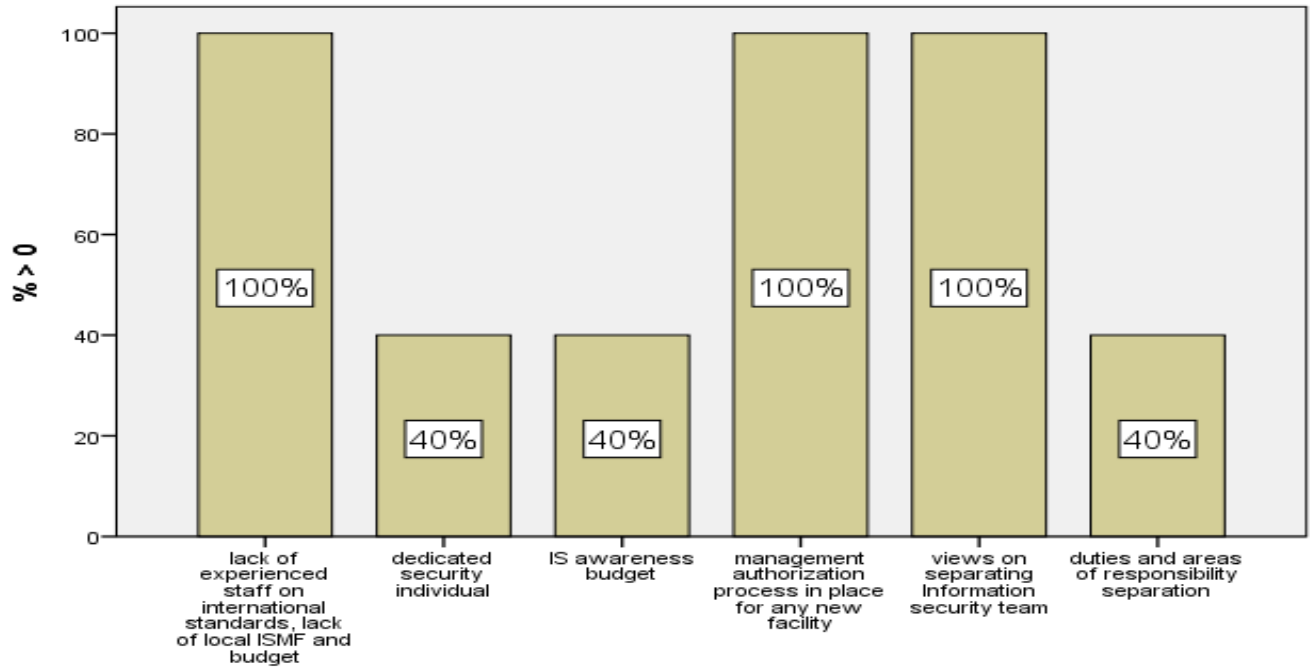


Figure 4-15 lack of experienced staff, lack of local ISM standard, and budget, dedicated information security individual(s), yearly budget for security awareness, management authorization, and separating security department.

As shown in figure 4-15 above, 40% of the banks have dedicated information security professionals with responsibility of assuring information security whereas 60% did not have dedicated expert.

Only 40% of the banks have allocated a yearly budget for staff information Security awareness program and technical training even though it is not enough whereas 60% they didn't allocate.

All of the surveyed banks, 100% have management authorization processes for new information processing facilities including all hardware and software use.

As shown in figure 4.-15 above, 100% of the those banks agreed on the idea of separating Information security team (department or unit) from other IT staffs structurally under IT department. In addition, in 40% of the banks duties and areas of responsibility has separated in order to reduce opportunities for unauthorized modification or misuse of information or services whereas 60% of the banks did not do same.

-Compliance

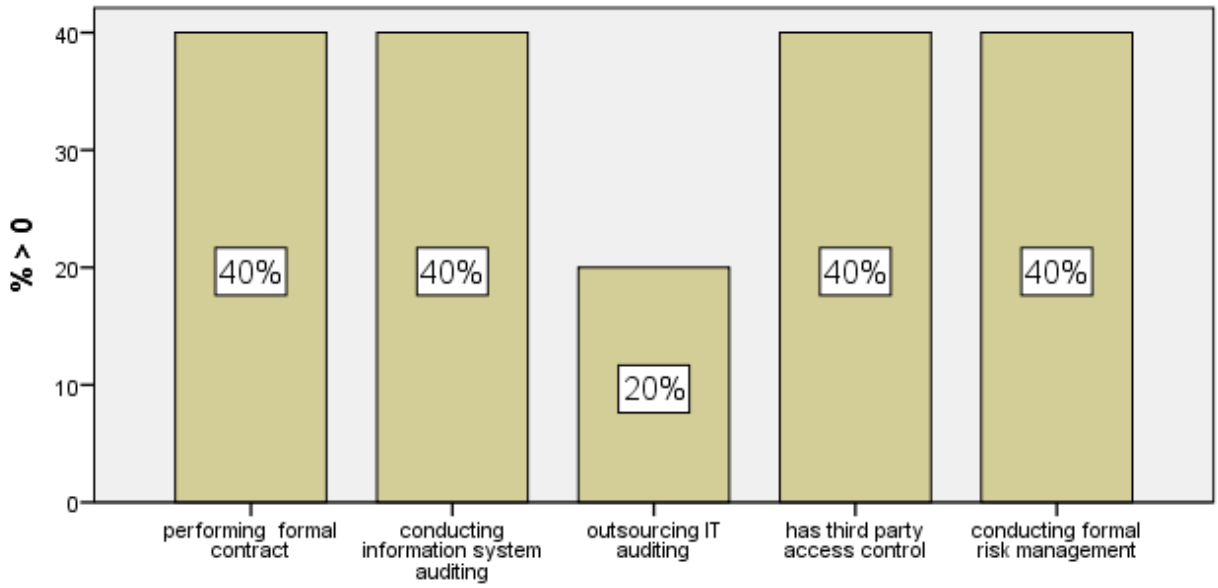


Figure 4-16 formal Contacts, auditing, outsource auditing, 3rd party access control, and risk management

As shown in figure 4-16 above, only 40% of the surveyed banks have made formal contract which refers to all the security requirements to ensure compliance with the Bank's security policies and standards.

In addition, 60% of those banks never conducting information system security auditing at all. Only 40% of them did it. And 20% of the surveyed banks outsourcing their IT Systems Security audit to third party and 20% do by themselves (internally).

-Risk management

As shown in figure 4.16 above, Risks from third party access to bank's information and IT resources is not identified and appropriate security controls are not implemented in 60% of those banks. In 60% the bank did not conduct formal risk management activity before developing an Information security policy.

-Asset Management

As shown in figure 4-17 below, only 20% of the surveyed banks have defined information asset inventory and classification scheme which assists in determining how information should be handled or protected.

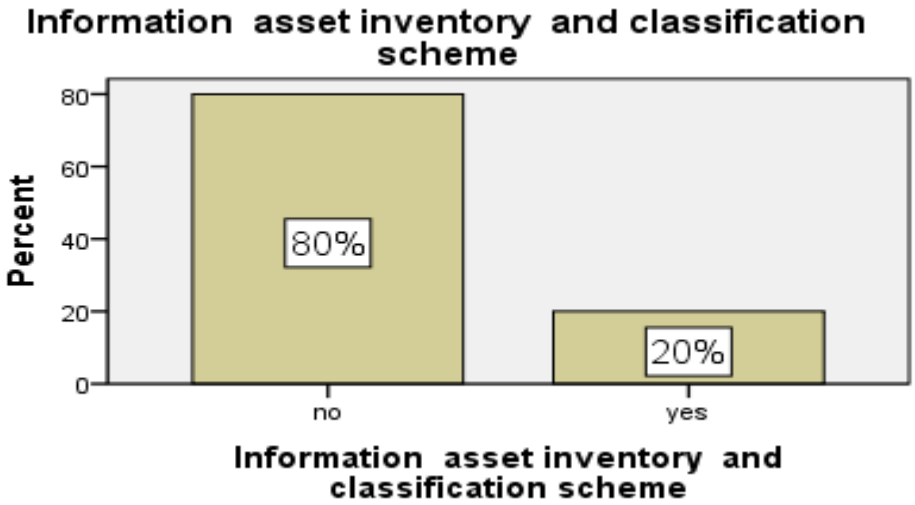


Figure 4-17 Information inventory and classification scheme

-Personnel Security

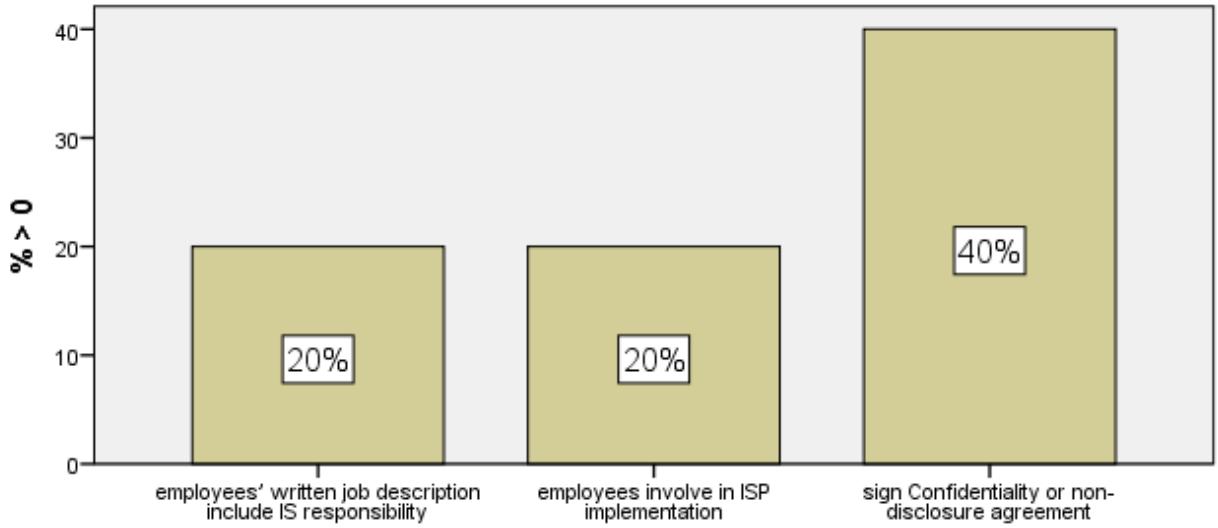


Figure 4-18 information security responsibility is included in job description includes, Information Security awareness for employees and third party

As depicted in figure 4-18 above, employees' written job description includes responsibility for information security in 20% of the surveyed banks. And 20% of the banks invite employees to participate in the development of information security policies in order to encourage a sense of ownership.

In addition, in 40% of those banks have confidentiality or non-disclosure agreement with employees as a part of their initial terms and conditions of the employment.

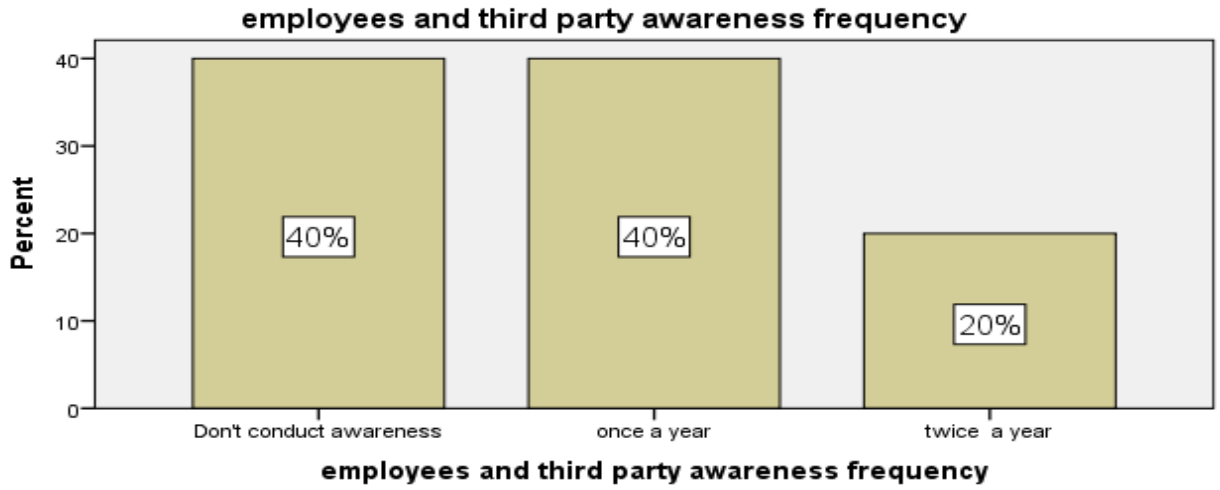


Figure 4-19 employees and third parties awareness

As shown in figure 4-19 above, in 40% of the banks surveyed, employees and third parties in banks didn't get training and updates on information systems security, while 40% replied that they do conduct training and awareness on IS security once a year and 20% twice a year.

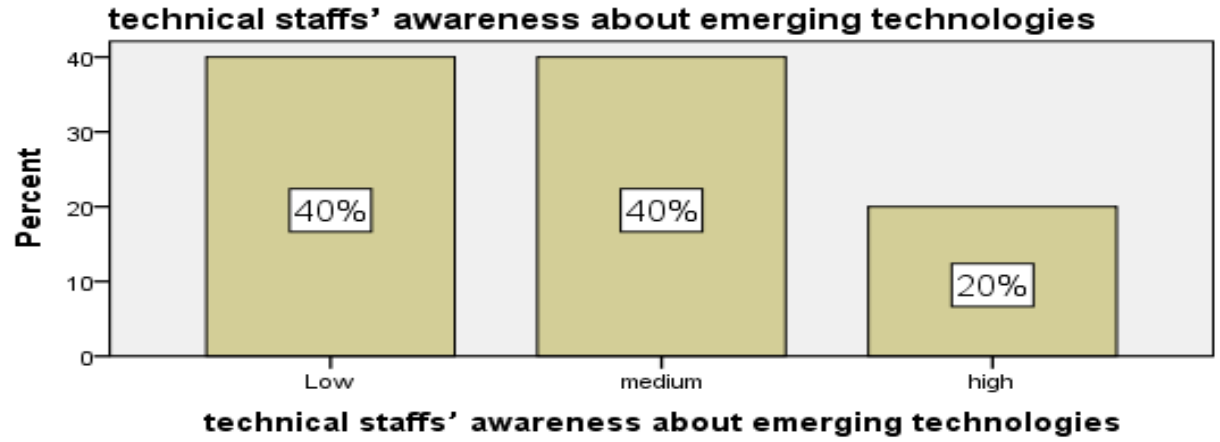


Figure 4-20 technical staff emerging technology awareness

As depicted in figure 4-20 above, technical staffs' awareness about emerging technologies and related control issues rated as low, medium , and high with 40%, 40% , and 20 % of the surveyed banks respectively.

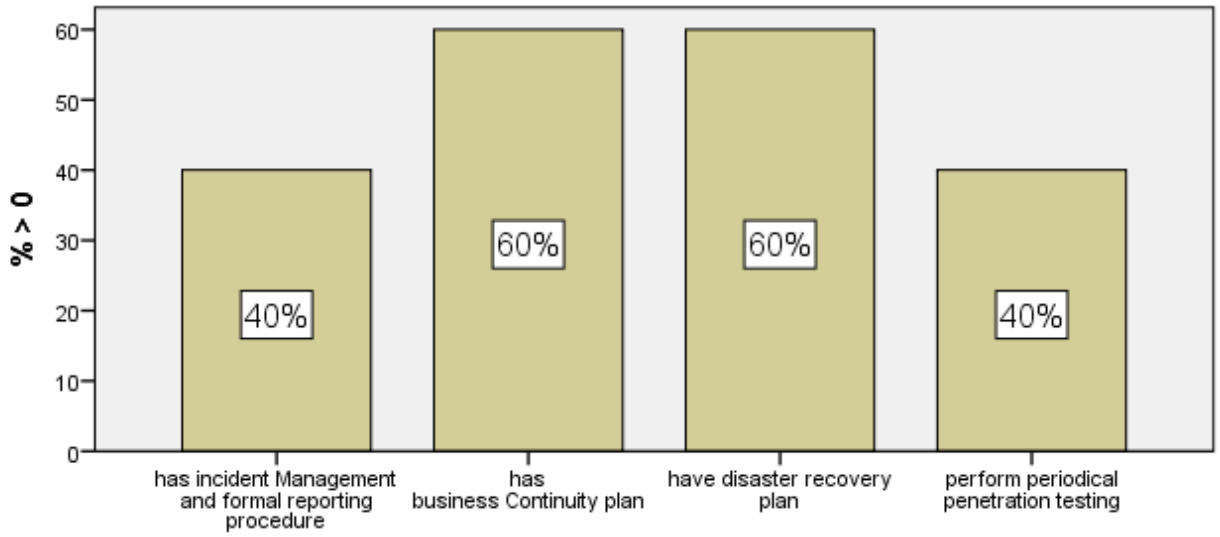


Figure 4-21 Incident management & formal reporting procedure, Business Continuity & disaster recovery plan, and Penetration testing

As depicted in figure 4-21 above, 40% of the surveyed banks have written incident management and formal reporting procedure to handle security incidents. But the remaining they don't have it. In addition, 60% of the surveyed banks have an approved Business Continuity and Disaster Recovery plan.

Only 40% of the surveyed banks perform periodical penetration testing of their infrastructure.

Implication

As we can see from the above graphs under administrative category, in general specking, surveyed banks are weak in designing and implementing security policies & procedures, standard usage, Stakeholders involvement, risk assessment, management support, personnel security, asset management, and staff awareness.

4.8. Summary of Controls

Controls are all those countermeasures or safeguards that are put in place in a bank and that make up the information security management system. Example of controls can be rules in the information security policy, a packet-filtering firewall, or a physical door with a lock.

All controls which are found in questionnaires are summarized into three categories namely; Administrative / Organizational, Technical, and Physical & Environmental controls. Moreover, some of the controls emerged from the empirical study are also classified under these categories.

➢ Administrative /Organizational controls

Administrative controls are those that try to affect the formal (e.g. by stating rules in a security policy) and informal parts (e.g. by increasing employee awareness via education and training) of information security. Main Administrative controls are:

- Information Security Policies, procedure, best practice, and guidelines
- Organizational security
- Education and training /awareness
- Incident Handling
- Business Continuity and disaster recovery Plan
- Asset management /Information Classification and inventory method
- Compliance (Legal and regulatory)
- Personnel security
- Internal and External Auditor
- Risk management and assessment process

➢ Technical controls

Technical controls are those that are installed and operated in the computer systems. Some administrative controls, like rules, can also be matched by technical controls e.g. enforce the rules, Access Control List. Main Technical controls are:

- Access Control
- System development consideration
- Communication and Operation Management
  - Antivirus
  - Automatic Patch Updates/ patch management
  - Backup
  - Cryptography/ Encryption
  - Firewall & Intrusion Detection System
  - Monitoring , logging and auditing

➢ Physical & Environmental controls

Physical controls are those that try to protect the bank's information security by physical means. For example, a guarded reception in an office building would be an example of a physical control aiming to keep the bank's physical security perimeter intact. Physical & Environmental controls are:

-Building Management System-BMS

- Door Access Control system
- Fire Protection and Alarm System
- Air conditioning system

- UPS
- Backup power/ alternate power source
- CCTV Camera

-Fence & Security guard

4.9. Comments from Respondent

Some comments and suggestions from employees of Information System in surveyed banks are listed below. They are obtained through open paragraph question at the end of the questionnaires.

-Giving Information System security training for all employees in bank is important.

- Security policy must be developed based on formal risk assessment result

4.10. Interview -Analysis of Views

The analysis of qualitative data is done using observer impression. Interview findings are described in terms of words, and are structured as per the interview questions, as follows:

- ISM Framework that the bank has employed and its drawback(s) and strength(s)
- problems that impede and success factors in the process of development and implementation of ISMS
- methods of security requirement identification prior to select best practices
- a kind of risk management methodology that banks have used
- Information security management structure

The aim of this analysis is to examine the different IT security managers' view and idea regards to the management of information security in bank the interviewees hold, as well as to arrive at condensed descriptions of these views.

The organization of this section is presented as follows: First, each interview question is presented along with a condensed text that describes each interviewee's view. Then, a final synthesis is made that integrates these views under each question.

4.10.1. Type of Standard a surveyed banks have employed

Question1. *If you have developed ISMS in your bank, what kind of standard or framework the bank employed in the process of ISMS development? If not developed ISMS, why? What is/ are the reason(s)?*

Interviewee 01

Interviewee 01 explained that there is no formal and compressive developed ISMS rather there are a fragmented policies and procedures that the bank applied to protect its information

asset. However, currently, the bank is on the position of initiation to develop and implement compressive bank wide ISMS. Information system department has initiated and prepared ISMS design and implementation proposal document and submitted to executive management team. As a result, the top management has established ISMS team. This team has prepared two documents viz, bank's ISMS team charter and Request For Proposal (RFP) for consultant and submitted to executive management team for approval. In addition, the budget has approved by the management and the team has got a direction from management to start the next phase.

In addition, interviewee 01 noted that the bank has decided to follow the ISO/IEC27001 &2:2005 standard because of the following reason:

- Since it is the base of our national security policy which was announced by Federal
    - Democratic Republic of Ethiopia on September 2011
- It has a compressive nature. So that it helps the bank to see as a whole and implement a complete ISMS based on bank's need.
- It is easy to understand by stakeholders
- It is widely used security framework in the world.

Interviewee 02

Interviewee 02 stated that for a long period of time there is no formal and compressive developed ISMS rather there were a fragmented policies and procedures that the bank has employed. However, currently, the bank is on the position of designing compressive banking ISMS based on ISO 27001 &2:2005 and COBIT. And the consultant service has been given to INSA. In addition, the counter team has established on the bank side and working with INSA's team. Moreover, following the ISMS designing and implementation project different teams has established by the bank such as IT audit and evaluation team, Penetration testing team, Cyber threat management and close hall team.

Interviewee 03

According to Interviewee 03 there is no a compressive IT security policy in the bank. However, currently there is an initiation form IT department to start develop and implement ISMS which compliance with the regulatory requirements of NBE and National information security policy.

Interviewee 04

Interviewee 04 noted that there is no formal developed ISMS rather there is non-formalized policies and procedures that the bank applied to protect its information asset. Because of the following reason the bank didn't yet design and implement compressive ISMS. These are: lack of ISMS understanding by top management, lack of motivations even within IT department, lack of budget due to less attention of top management, and lack of domain experts are some of the challenges.

Interviewee 05

Interviewee 05 stated that there is no formal developed ISMS rather there is non-formalized and fragmented policies and procedures that the bank applied to protect information asset. The bank didn't yet design and implement compressive ISMS due to the following reason. These are: the bank is new, lack of ISMS understanding by top management, and lack of domain experts are some of the challenges in this bank.

4.10.1.1. Summary of views

All Interviewees of the five banks explained that there is no formal and compressive developed ISMS in their bank. However, from the five banks two banks have already planned and started the designing and implementing of ISMS project. In addition, one bank is at initiation stage to motivate the management for ISMS project establishment whereas the remaining two banks do not show any motivation.

4.10.2. Strengths and drawbacks of standards that banks employed

Question2. *What is/are the drawback(s) and strength(s) of the standard that you have employed in ISMS development?*

Interviewee 01 and Interviewee 02

Interviewees 01 & 02 explained that since the bank is in its first phase of designing and implementing of ISMS project, it is difficult to speak about the strengths and weakness of the standards.

Interviewees 03, 04, and 05

Interviewees 03, 04 & 05 have also similar explanation that since the bank did employ yet any standards, it is difficult to talk about it's the strengths and weakness.

4.10.2.1. Summary of views

Surveyed banks are not in the position of telling the strengths and weakness of any standard since they do not come across the designing and implementation of ISMS project.

4.10.3. ISMS Development and Implementation project impending problems and success factors

What are the negative (impending) elements of ISMS development and implementation process? And what are the critical success factors for a successful development and implementation of ISMS?

Interviewee 01

- ***Problems***

According to the interviewee 01 there are different challenges that delayed the designing and implementing of banking wide ISMS. To recall some of them are: lack of ISMS understanding by top management, lack of employee motivation, lack of budget due to top management low attention, and lack of domain (standards) experts were some of the challenges in this bank.

- ***Success factors*** *(based on interviewee opinion)*

According to the interviewee 01 the identification of the information assets of the bank is one of the critical success factors for the efficient and effective implementation of information security in bank. Interviewee 01 justification is that if you don't know your asset it is difficult to identify the risks and threats. Even you don't know how protect them. Further, board level direction, active involvement and support of Top management for quick resolution of Information Security Issues is very important.

Moreover, interviewee 01 explained that the integration between business and Information Security, Alignment of Information Security mechanisms with Organizational Goals and Objectives, Information Security planning and assessment of new technologies before installation, and employees awareness are the main success factors.

Interviewee 02

- **Problems**

Interviewee 02 has listed out the problems that the IT department has faced for a long period of time in assuring information security process. These are:

- There is no local ISM Framework or guidance in the bank and International standards are not satisfactory for our country.
- Work overlap in IT department- one IT personnel has assigned for multiple tasks for example, he/she works on operation and security. This generalist approach will bring many problems such as: security will be compromised, employee dissatisfaction, decrease employee productivity …etc.
- Information security as a discipline is not given by Ethiopian Universities and colleges. As a result, graduated students have started learning about security when they hired in the bank.
- Attention for security was not given by top management
- No incentives to attract experienced information security staffs
- There was no investment for a long period on security until CORE banking project has started.
- No well-organized security team until CORE banking project has started.

- **Success factors**

According to the interviewee 02 CORE banking project has brought much contribution to information security. For example, CORE banking solution has integrated Security Management System module (SMS) which governs the user access privileges centrally. In addition, purchasing of new security management hardware and software products is the effect of CORE banking project. Generally, CORE banking solution is an opportunity of information security management improvement in bank industry.

In addition, interviewee 02 underlined that security awareness and commitment of employees is the main key success factor in ISMS designing and implementation process in addition to the following ones. These are: Holistic approach, motivated employees, Top management's commitment and ability to put policy into practice, and well-organized information security team.

Interviewee 03

- **Problems**

  According to Interviewee 03 the following problems are affecting information security management process. These are:

  - Information security as a discipline is not given by Ethiopian Universities and colleges. As a result, graduated students have started learning about security when they hired in the bank.
  - There is no information security management framework or guidance in the bank.
  - Work overlap in IT department- one IT personnel has assigned for multiple tasks.
  - Attention for security was not given by top management in the past.
  - No incentives to attract experienced information security staffs
  - There was no investment for a long period on security until CORE banking project has started.
  - There was no well-organized security team
  - There is no testing environment.

- **Success factors**

The third interviewee (03) tried to list out major success factors of ISMS development and implementation. These are: accurate analysis of preceding security situation, active employee participation, active project members and appropriate project organization, backing from top management, Customer participation for example in case of mobile and internet banking, and documented security processes.

Interviewee 04

- **Problems**

  Interviewee 04 identified the following problems which affects information security assurance process. These are:

- Information security as a discipline is not given by Ethiopian Universities and colleges. As a result, graduated students have started learning about security in the bank.
- There was no information security management framework or guidance in the bank.
- Work overlap in IT department- one IT personnel has assigned for multiple tasks.
- Attention for security was not given by top management in the past.
- There was no investment for a long period on security until CORE banking project has started.
- There is no well-organized security team

➢ **Success factors**

According to interviewee 04 the following are critical success factors of ISMS development and implementation project. These are: accurate asset identification and risk analysis, insight and knowledge about security, integration with existing management systems, and top management awareness and commitment. In addition, interviewee 04 argued that threat by itself will be success factors since it triggers the top management and IT staffs.

Interviewee 05

➢ **Problems**

According to interviewee 05 the main challenges are:

- Work overlap in IT department- one IT personnel has assigned for multiple tasks for example, he/she works on operation and security. This generalist approach will bring many problems such as; security will be compromised, employee dissatisfaction, decrease employee productivity …etc.
- Information security as a discipline is not given by colleges. As a result, graduated students have started learning about security in the bank.
- There is no security awareness creation program in the bank.
- No clearly defined Ownership and accountability, at all levels

➢ **Success factors**

The fifth interviewee is in the position that technology does not solve all problems. People are the key factor. If people do not understand why it is necessary for the business, and then it doesn't work. It doesn't matter what technology you have - there is no technology that can protect you against human beings. The project members and other employee's ability to see the "full picture" is the underline point of the interviewee 05.

The ultimate goal for information security efforts is to reach information security awareness among the employees. As Interviewee 05 puts it "You can buy any number of machines, but if you do not have employee awareness, they'll post a password on the edge of the screen".

4.10.3.1. Summary of views

- ***Problems***

The main challenges in designing and implementation of ISMS which are explained by the interviewees are listed below:

- Lack of top management understanding about ISMS development and implementation project
- Lack of employees' information security awareness
- Information security as a discipline is not given by Ethiopian Universities and colleges.
- Work overlap in IT department- one IT personnel has assigned for multiple tasks. For example, he/she works on operation and security.
- Budget constraint due to the nature of ISM, since it doesn't have direct investment return.
- Lack of domain expert (experts in different standards)
- There is no local ISM Framework or guidance in the bank.

- ***Success factors***

The summarized success factors as explained by the five interviewees are:

- having the continuous, unshakeable and visible support and commitment of the bank's top management
- Financial capability or the budget that a bank allocates for ISMS development and implementation process.
- Holistic approach of ISM
- Analytic capability or risk analysis ability
- Communicative capability, and awareness creation ability
- ability to put policy into practice
- Security objectives and activities shall be based on business objectives and requirements.
- Clearly defined ownership and accountability, at all levels
- documented security processes
- insight and knowledge about security

4.10.4. Security requirements identification

How the bank identifies its security requirements prior to select best practices or controls? Does it use models? If so, what are the drawbacks and strengths of the model that you have employed for security requirement identification?

Interviewee 01

Interviewee 01 has noted there is no predefined security requirements identification model that aids the need assessment process before selecting controls. The controls are selected by the general understanding and expert's experience, and venders or contractor advice. However, Interviewee 01 also adds, the requirement identification should follow some models since the technology is dynamically changed and it also should be based on business objective.

Interviewee 02

Interviewee 02 has also argued the same as that of interviewee 01. That is, there is no a predefined security requirement identification models. However, Interviewee 02 noted that the bank employed general knowledge and experience of experts, using ISO standards, INSA's recommendation, and by adopting national information security policy.

Interviewee 03 and Interviewee 04

Interviewees 03 and 04 noted that there is no a predefined security requirement identification methods or models rather the bank employed general knowledge and experience of IT experts, and using national information security policy as a reference.

Interviewee 05

Interviewee 05 explained that there is no a predefined security requirement identification steps or models rather the bank employed general knowledge and experience of experts, picked up best practice from different standards and testing it, and adopting national information security policy.

4.10.4.1. Summary of views

Form the above five surveyed banks' interviewees explanation there is no a predefined security requirement identification methodology or model. All surveyed banks employed the combination of general knowledge and experience of experts, ISO standards, INSA's recommendation, and by adopting national information security policy.

4.10.5. Risk management methodology

What kind of IT risk management methodology you have employed?

Interviewee 01

According to interviewee 01 unless otherwise the bank knows its asset and the level of protection needed security may not be assured. Thus the information asset classification

scheme should be based on potential financial consequences of a security breach. Unfortunately, the bank does not have IT risk management methodology. However, Interviewee 01 suggests that one should approach IT risk management by following these steps strictly: a) identifying products/services that generate material revenue streams to the bank; b) identifying potential scenarios of security breaches; c) identifying what types of risks they cover; d) evaluating current security in the IT systems; e) deciding on the needed security level based on the financial risk exposure; and f) Implementing the security level as technical controls.

Interviewee 02

Interviewee 02 believed that to achieve information security objective, the IT department of the bank must work closely with business departments or operations to create effective risk analysis and protection mechanisms. Further, a holistic approach in risk analysis process is required. However, there was no IT risk management methodology for a long period but following the CORE banking project the IT risk management team has established and works on IT risk management even though it is in infancy stage.

Interviewee 03

Interviewee 03 said that a holistic approach to risk analysis is required. Unless otherwise the bank performed risk analysis by viewing the whole picture based on its business interaction security assurance may not be effective. Thus, Interviewee 03 mentioned some points that the bank followed in risk assessment process. These are: information assets identification, risk identification, risk analysis, risk evaluation, and controlling risk.

Interviewee 04

Interviewee 04 explained that there is no a predefined IT risk management in the bank. Rather risks are identified and managed based on expert's knowledge and experience.

Interviewee 05

Interviewee 05 observed that there is no predefined IT risk management methodology. Risk management is handled by business risk and compliance department of the bank. In essence, Interviewee 05 argues that information security should be based on business processes, economics, and management of risks. a holistic approach in risk analysis process is essential. Thus, first bank's asset that support business process must be identified, risk assessment be

performed, risks must be prioritized based on their severity level, appropriate (economical) controls must be selected and implemented.

4.10.5.1. Summary of views

Most of surveyed banks do not have a predefined IT risk management methodology. What I have observed from the five banks' interviewees is that a holistic approach in risk analysis process is required. Each bank must approach risk analysis in all-inclusive manner. This means that one cannot only do a risk analysis of one system as a separate entity if it is interconnected with many other systems, because of the inherent dependencies. In addition, the following steps will be taken as risk management methodology. These are: information assets identification, risk assessment/ identification, risk analysis, risk evaluation, and controlling risk.

4.10.6. Information Security Management Structure

What is your opinion about the pros and cons of separating Information security management team from other IT staffs structurally in IT department?

Interviewee 01

Interviewee 01 agreed that the structure of IT department has a great contribution in information security management. However, in the bank, the IT department follows the generalist principle to use the experts effectively. But this principle has brought many challenges to the bank. Because the generalist approach is prone to attack, employees' dissatisfaction, turnover also increases. Interviewee 01 recommends that bank shall have separate streams or verticals to manage IT in some form or the other, such as: application and infrastructure management, systems management and IT security. The primary responsibility of these groups is to manage their individual areas in terms of delivery, ensure compliance to the IT policies of the bank.

In addition, Interviewee 01 has noted that sometimes the role of the security consultant is to say to top management what the information security officer has tried to say for a long time. As it turns out, sometimes top management is more open to the external advice from an information security consultant than from the internal advice from a lower part in its own bank.

Interviewee 02

Interviewee 02 agreed that the structure of IT department has a great contribution in information security management. For example the generalist principle prone to many problems as mentioned above by interviewee 01. However, generalist approach may work within related areas such as network area, and application area. Because, rotating experts within the same area can be advantageous but generalist approach is not applicable from

security aspect. Segregation of duty is very important. Thus, the bank must separate the IT security department from other IT departments such as Application system and Technical support, MIS, Application Development and Customization, and network infrastructure management. And Interviewee 02 adds that IT security department has further divided into three units such as Application security, infrastructure security, and physical & environmental security.

Interviewee 03

Interviewee 03 also agreed that the structure of IT department has a great contribution in information security management process. Currently, the bank has tried to separate the IT security department from other IT departments structurally but it is not in staff organization.

Interviewee 04

Interviewee 04 agreed that the structure of IT department has a great contribution in information security management. However, in the bank, the IT department follows the generalist approach even though security department structurally separate. The IT department has the following divisions: networking, application, helpdesk, IT security, and e-banking and development divisions.

Interviewee 05

Interviewee 05 agreed that the structure of IT department has a great contribution in information security management. The generalist principle will prone to many problems such as employee dissatisfaction, turnover, and system compromise. However, generalist approach may work within related areas such as network area, and application area. Because, rotating experts within the same area can be advantageous but generalist approach is not applicable from security aspect. Segregation of duty is very important. Thus, the bank shall separate the Security division from other IT departments such as system division, support division, network infrastructure management division, and E-banking division.

4.10.6.1. Summary of views

All interviewees have agreed on the point even though the real structure of their IT department and principles is varying. The structure /organization of IT department have a great contribution in information security management. If the bank's IT department follows the generalist principle to use the experts effectively, as they thought, then it will bring many challenges to the bank. Since the generalist approach is prone to attack, employees' dissatisfaction, turnover also increases. So, as all Interviewees recommended every bank shall

have separate streams or verticals to manage IT department in some form or the other, such as Application system and Technical support, IT security, MIS, Application Development & Customization, and network infrastructure management. If they organized in such a way they know that the primary responsibility of these groups is to manage their individual areas in terms of delivery, and ensure compliance to the IT policies of the bank.

4.11. Summary of findings

The results, presented in summary below indicate how the interviewed experts perceive and perform information security management in their banks. Focus is to arrive at an integrated view based on their perceptions and activities rather than trying to emphasize the differences among them.

- All Interviewees of the five banks explained that there is no formal and compressive developed ISMS in their bank.
- The main challenges in designing and implementation of ISMS project are:
    - Lack of top management understanding about ISMS designing and implementing project
    - Lack of employees' information security awareness
    - Information security as a discipline is not given by Ethiopian Universities and colleges in Ethiopia.
    - Work overlap in IT department- one IT personnel has assigned for multiple tasks. for example, he/she works on operation and security.
    - ISM budget constraint
    - Lack of domain expert (experts in different standards)
    - Lack of local ISM Framework or guidance in the bank

- The summarized major success factors which are explained by the interviewees are:
    - Holistic approach of ISM
    - Analytic capability or risk analysis ability
    - Having continuous, unshakeable and visible support and commitment of the bank's top management.
    - Financial capability or the budget that a bank allocates for ISMS project
    - Communicative capability and awareness creation ability
    - Ability to put policy into practice
    - Ownership and accountability, at all levels
    - documented security processes
    - insight and knowledge about security
- There is no a predefined security requirement identification methodology or model. All surveyed banks employed the combination of two or more sources such as: general knowledge and experience of experts, ISO standards, INSA's recommendation, and by adopting national information security policy.

- None of surveyed banks have IT risk management methodology. They have agreed on the need of it and a holistic approach in risk analysis process is required.
- All interviewees have agreed on the point even though the real structure of their IT department and principles is varying. The structure /organization of IT department have a great contribution in information security management. If the bank's IT department follows the generalist principle, it will bring many challenges to the bank such as attack, employees' dissatisfaction, and turnover also increases. So, segregation of duties and responsibilities is very essentials.

The researcher found that despite the seriousness of the nature and scope of the security threats posed by the environment vary; surveyed banks are under-prepared to mitigate the threat. In addition, there appears to be a lack of understanding of how banks should design and implement a compressive information security policy, and how security requirements are identified. The framework described herein could be utilized in an effort to effectively implement holistic and successful ISMS.

CHAPTER FIVE

THE PROPOSED ISM FRAMEWORK

To secure a bank's information asset the entities or organizations degree of interaction to the bank and business process IT risk level should be known prior to any business agreement is made. Nowadays, information security is not only a technical issue, but also a management and business issue as well.

The literature review, questionnaire and interview findings and the researcher's own experience show that there is no local ISM framework that aid in development and implementation of ISMS to secure data in banking industry in Ethiopia.

Therefore, based on insights gained from the analysis of literature on various frameworks such as ISO/IEC27k series, COBIT, PCI DSS...etc., data analysis of interviews and questionnaire findings, and the student researcher own professional experience ISM Framework has been proposed. The proposed ISM Framework has two major components viz; requirement identification mechanism and Counter measures.

In requirement identification mechanism the student researcher used the combination of two models such as: Entity Relation Model (ERM) and ISMS process Model to identify a bank's information security requirements prior to select best practice or controls. The process is supported by a template which is developed by the student researcher.

ERM is employed to identify the entities which have interaction to a bank and information flow among them whereas ISMS process model is employed to guide the bank's information security requirement identification and best practice (control) selection and implementation process.

In addition, the researcher's own defined template or tool is employed for easy understanding and documenting the detail security requirement identification and controls selection process.

Banks in Ethiopia have different goals, strategies, organizational cultures and structures. Consequently, the ideal management system and the way to achieve it will differ among banks. Thus, this study proposed a framework instead of a comprehensive information security management methodology.

5.1 Objectives of this ISM Framework

- To support the attainment and realization of three information security objectives across banks: Confidentiality, Integrity and Availability of information.
- To provide a framework that assists banks to achieve information security in banks.

5.2 Proposed Organizational Structure of IT Department

The structure of IT department has a great contribution in information security management. All surveyed banks have agreed on this point and list out some limitation of generalist approach. For example, the generalist approach is prone to attack, employees' dissatisfaction, turnover also increases.

Banks may have separate streams to manage their IT in some form or the other, such as hardware Technical support, System and Application support, MIS, System Development and Customization, Information System security, and network infrastructure management are among others. The primary responsibility of these groups is to manage their individual areas in terms of delivery, ensure compliance to the IT policies of the bank. The scope of this section is Information system Security department /unit.

The bank's IT security department itself might have three sub departments or units which has flat structure viz, Network / infrastructure security, Application security, and Physical & Environmental security (figure 5-1). This kind of segregation will bring employees satisfaction, profound knowledge and skills on their focus area, and aids to build confidence. In turn, these all will have a great contribution on security assurance process in the bank.

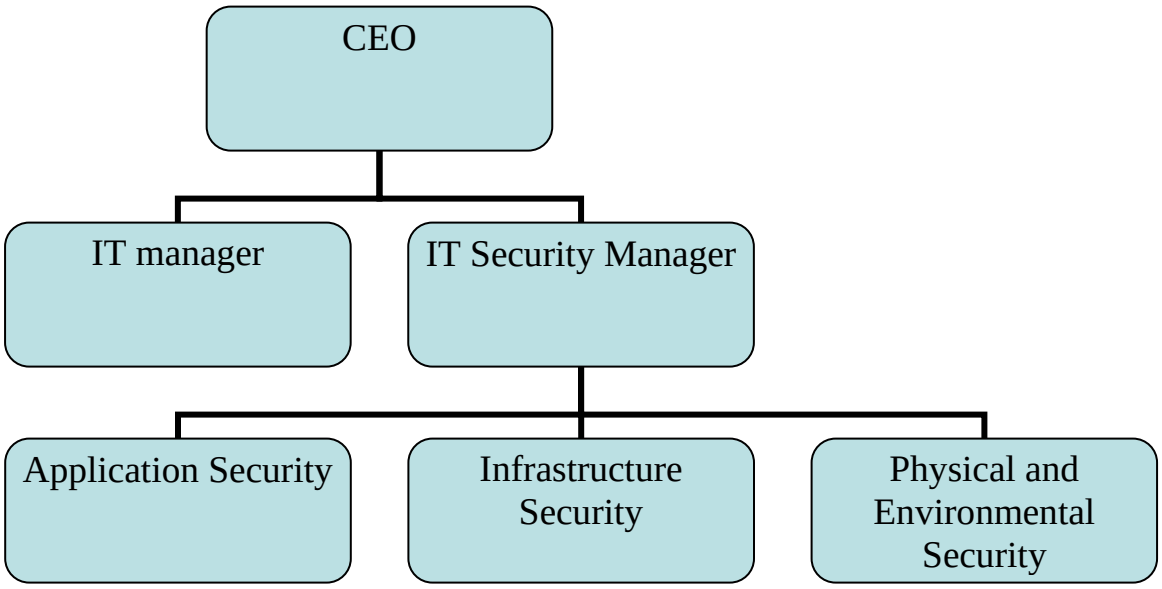


Figure 5-1 ISM Structure

Both IT manager and IT security manager are directly reports to Chief Executive officer, in turn to higher officials or board. The IT Manager of the bank is responsible for secure operation of the overall bank's system. All of the operational staff, for example, System

Administrators, report directly to the IT Manager. There are other departments under IT manager like network infrastructure, hardware Technical support, System and Application support, MIS, System Development and Customization. The IT Security Manger is responsible for enforcing security policy, compliance, business continuity and incident response activities, penetration testing, preparing security awareness creation program, and auditing. This structure ensures that operational staff will not easily be able to avoid security for convenience in operations or additional functionality against the security policy.

5.3 Risk Assessment and Management Methodology

5.3.1 Risk Assessment

To identify a risk a bank might want to adopt or adapt any one of the existing risk assessment and management methodologies in the domain. The methodology can assist the bank in identifying detailed risks in a bank information security management process. Of any kind, the risk assessment methodology should include at least the following steps. These are: asset identification, risk assessment (identification), risk analysis and risk evaluation / measurement.

5.3.1.1 Information Assets Identification

As defined in ISO/IEC 27001-2 (2005) “Asset is anything that has value to the organization”. Assets are an integral to the risk assessment process. Since security risk assessment is a precondition to protect an asset. When determining the assets, the bank must know detail the criticality or value of an asset. For example, for a physical asset (e.g. server) the value of the asset could be determined at the replacement cost, but there are a variety of other factors that need to be considered including, cost of unavailability of service provided and loss of reputation or goodwill, etc. It is important that all costs / values are considered.

Physical inventories of equipment and the data they host will help the bank to identify critical assets. There are two methodologies for creating a complete inventory: service based and hardware based (George et al., 2012).
A service-based inventory establishes a hierarchy of assets, starting with a top-level service, branching into the information assets that support it, branching again into the assets that support them, and so on.

The information asset identification process should at least identify:

- The bank’s information assets such as:
  Policies, procedures, guidelines, user manuals, Organizational chart, Function descriptions, Business applications, The data used by business applications and flow , Roles and Authorization matrix, Operating Systems, Database management systems,

IT utility programs, The existing network infrastructure, The communication links between the IT systems and the outside world, The hardware in use (e.g routers, firewalls, servers etc.).

- The owners of these assets
- The value and sensitivity of information assets
- The threats to those assets
- The vulnerabilities that might be exploited by the threats and
- The implemented security controls.

The best way for a bank to know its assets and protect them from attack, including from insiders, is to conduct a risk assessment. A risk assessment will teach a bank about the types of data its systems process, who uses the data, and where it is stored. (George et al., 2012).

5.3.1.2 Risk Assessment -Identification

The risk assessment is a process to identify the risks and assess the damage it could cause. The end result of a risk assessment is justification of any control or safeguards that need to be implemented to mitigate the risk to an acceptable level.

Risk identification is the determination of threats and vulnerabilities that could lead to an adverse event. The focus is on the nature and source of the risk such as:

- What could happen or go wrong?
- How could it happen?
- Why can it happen?
- Who or what can be harmed?

A combination of the following methods and techniques may be used to carry out the risk assessment: Interviews, Walkthroughs, Workshops, Questionnaires, "Computer-assisted audit techniques" (CAAT) (e.g. vulnerability scanning), and Network penetration testing.

5.3.1.3 Risk Analysis

Once the risk against any asset is identified, the risk is analyzed based upon two factors, namely, likelihood of risk materializing and the Consequence of risk materialization to the bank.

5.3.1.4 Risk Evaluation /Risk Measurement

Risk measurement is the next critical stage after identification and analysis of risks and it is concerned with quantifying the extent of the bank's risk exposure.

5.3.2 Controlling Risks /Risk Management/ Risk Treatment

The end result of a risk assessment is justification of any control or safeguards that need to be implemented to mitigate the risk to an acceptable level. The process of selecting controls or countermeasures will complete the Risk Management process.

5.4 Major Components of Proposed ISMF

The outcome of this study is a conceptual framework which is a comprehensive information security management framework that comprises of two components. These are:

- ***Requirement identification mechanism*** which is the combination of ERM (Entity Relation Model which is used to identify organizations and their interaction to a bank), ISMS Process model, and a template.
- ***Counter Measures*** **–**policy ,procedure, guideline, and controls

5.4.1 Requirement Identification Mechanism

The five surveyed banks' interviewees (see section 4.10.4.1) explanation indicates that there is no a predefined security requirement identification methodology or model. Currently, all surveyed banks employed the combination of general knowledge and experience of experts, INSA's recommendation, and by adopting national information security policy. In addition, available standards lack clear steps in security requirement identification. Thus, the student researcher proposed the combination of three tools namely, ERM, ISMS process model, and template as a security requirement identification method.

5.4.1.1 Entity Relationship Model (ERM)

ERM is employed to identify and represent inter entities (organizations which have interaction with a bank) and intra entities (departments or processes which have interaction with IS Process within a bank). In addition, this ERM is used to define information flow (in one way or two ways communication) between business entities (Michael, 2007). Simply it helps to model the entities aspect of ISM Framework.

5.4.1.2 ISMS Process Model

After entities are identified using ER-model the ISMS process Model (which is developed by Fredrik, 2005) is employed to identify potential risks and threats, designing a solution or select the counter measures, and to produce the implementation document. The ISMS process model describes the stages and the important activities involved in detail.

This model has three stages as stated by Fredrik (2005) such as Evaluation stage, Formation Stage and implementation stage (Figure 5-3).

5.4.1.3 Template

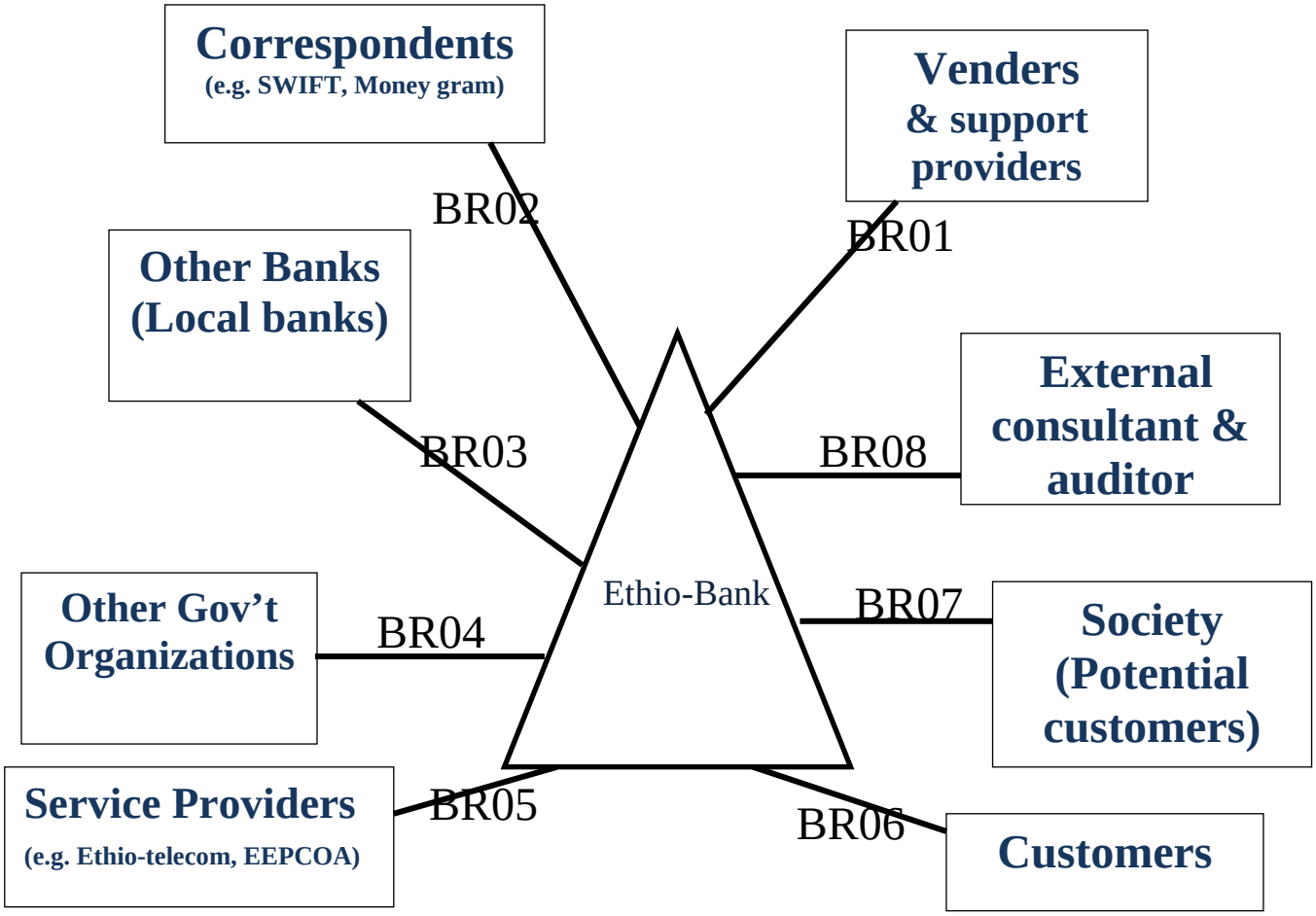
ISMS process model is supported by the template which is designed by the researcher for easy understanding and documentation purpose. The detail will be presented in the next section.

5.5 The Design of Proposed ISM Framework for Banking System

The proposed ISM framework can be used as a starting point by banking sector to manage information security in developing and implementing ISMS to protect banking information assets from the threats identified in literature reviews, interview and questionnaires of the study. This framework is an integration of available standard components discussed and derived from literature review. Nevertheless, the suggested framework is still a general approach to information security management program, it needs to be reviewed by professionals and tested in the real banking environment. As each bank's environment is different and additional components might be required. Since Framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful (ISO2001-2, 2005).

ISM Framework has a great contribution in ISMS development even though it is a time consuming process, but it is a necessary task to secure operations of any Information System. This paper demonstrated the ISM Framework using ISMS Process model, ER-model and template.

5.5.1. ERM- Different Entities Inter relationship to Ethio-Bank (a model Bank)



- BR = Business Relationship (interaction)

Figure 5-2 Different Entities Inter relationships to Ethio-Bank

5.5.1.1 The description of each entity or "Responsible Party"

ER-diagram is used to show the trust relationship or interaction between entities (figure 5-2). It is also used to identify a type of information assets, resources required for business process, level of interaction through the communication channel. Information should be protected at processing, dissemination or moving and at rest. The following are list of entities with their description:

- ***Vender***: A vendor is any person or company that sells goods or services to bank. On another words, it is an external entity to the bank that is typically responsible for compliance with the ISMS by way of a contractual agreement that contains clauses

requiring security of bank information and the regulation of access to a bank's information assets.

- ***Correspondent:*** A type of financial institutions which has a business objective and agreement with bank. For example, SWIFT, Money Gram, Express money...etc.
- ***Other Banks (Local Banks):*** A type of finical service providers which has a business objective and agreement with Ethio-Bank. For example, the relation between CBE with NBE.
- ***Other Gov't Organization:*** Bank regulations are a form of government regulations which subject banks to certain requirements, restrictions and guidelines. This regulatory structure creates transparency between banking institutions and the individuals and corporations with whom they conduct business, among other things. E.g Public Financial institution Agency's orders.
- ***Service Providers*****:** these are used in two contexts within the ISMF. These are:
    - An Internet Service Provider (also known as ethio-telecom) is a company that offers subscribers access to the internet or provide banks with an internet connection.
    - An Electric power Service Provider (also known as an EEPCOA) is a corporation that offers electric power to banks.
- ***Customers:*** For a bank, a customer is a person who is utilizing one or more of the services provided by the bank. A customer is a person through whom the bank gets an opportunity to make an earning in return to the service they can provide the customer with.
- ***Society*** **:** national and international society

  A society, or a human society, is a group of people related to each other through persistent relations, or a large social grouping sharing the same geographical or virtual territory that has a great impact on the continuity of a business, the bank. The potential customer of bank will born form the society. It will be interact with the bank via banks service or consuming information form bank's web site.
- ***Consultant*****:** anyone who gives professional advice or services related to information technology to the bank for fee. Consulting is most often used when a bank needs an outside expert opinion regarding a business decision. For example, a bank seeking to design and implement its CORE banking solution may look for a consultant familiar with the technology.
- ***External Auditor:*** an external auditor is an individual or auditing company that inspect, analyze and rate the financial (or IT services) operations and practices of banks for fee.

5.5.1.2 Stakeholders' Business Relationship or interaction to Ethio-Bank

- *BR01* is a Business Relationship (interaction) between venders and support providers to Ethio-bank
- *BR02* is a Business Relationship (interaction) between Correspondent and Ethio-bank

- *BR03* is a Business Relationship (interaction) between Other Banks (Local banks) and Ethio-bank
- *BR04* is a Business Relationship (interaction) between Other Gov't Organization and Ethio-bank
- *BR05* is a Business Relationship (interaction) between Service Providers such as ethio-telecom, and EEPCOA to Ethio-bank
- *BR06* is a Business Relationship (interaction) between customers and Ethio-bank
- *BR07* is a Business Relationship (interaction) between Society (Potential customers) and Ethio-bank
- *BR08* is a Business Relationship (interaction) between Consultant & external auditor and Ethio-bank

5.5.2 ISMS process Model

This model has three stages as described above (section 5.4.1.2). These are: evaluation, formation, implementation stages and feed back

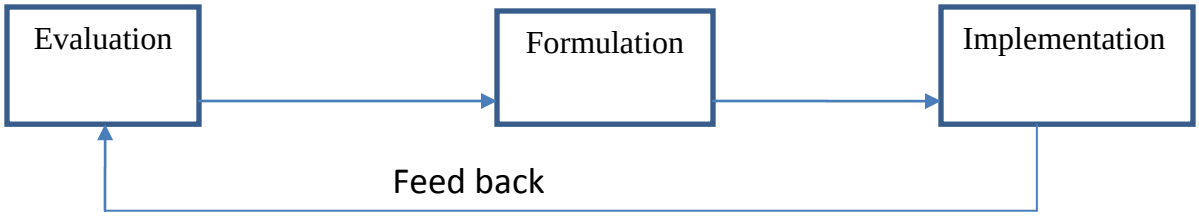


Figure5-3 the model divides the ISMS process into its sub-processes

- ***Evaluation stage***: What is the subject of evaluation? What types of activities are generally associated with an evaluation? What does an evaluation result in?

  The evaluation stage includes everything it takes to assess the current situation vis-à-vis information security management in the bank. It takes into account not only the administrative / organizational security issues, but also the technical (IT) security issues. The main results (output) of the evaluation stage are reports of vulnerabilities and deficiencies in relation to information security.
- ***Formulation stage:*** The formation stage takes these reports as its main input. And also adds knowledge about the bank, its business processes, culture, etc. The goal is to design and develop solutions tailor-made to the bank that will remedy any vulnerabilities and deficiencies in the current situation. The formation stage is largely analytical.
- ***Implementation stage:*** The implementation stage takes the solutions from the conceptual level and makes them work in the organization. It entails for example installing and configuring technical security mechanisms as well as information security education and training to employees.

- ***Feedback:*** Once implemented, the ISMS is in operation and it starts to generate feedback information to the next iteration – as input into the new evaluation phase. Now, let us examine each of these stages more closely.

A. Evaluation Stage

The goal of the evaluation stage is to assess the current information security situation of the bank. This evaluation takes into account not only the administrative security issues, but also the technical (IT) security issues. Before any fruitful evaluation take place, ISMS development team of a bank needs to gather some information (table 5-1). That is, information gathering based on business objective and IT strategies of the bank. There should be pre-evaluation task.

Parameters that are considered in the template are:

- ***BRID***: Business Relationship Identification
- ***Description***: tells the involved entities in the given relationship or business process.
- ***Channel***: means of communication between Ethio-Bank and any entities or departments within a bank. It determines mode of interaction among entities: viz, User to system, user to user (Manual via messenger) or System to system (electronically like edge router to edge router).
- ***Inputs***: any documents like business objective, and channels. Inputs may differ in each stage.
- ***Procedures***: activities that are performed in each stage of ISMS process model
- ***Outputs***: the result of each stage after processing the inputs.

BRID	Description	Channels **(Means of communication)**	Inputs	Procedures	Out put
BR01	A business relationship between Ethio-Bank and venders	paper, email, electronically	- Business strategy - IT strategy - business Process knowledge - Information assets -Public Financial institutions Agency's orders -Directives issued by the NBE -Policies and procedures of the bank -Directives issued by the bank -National Information Security Policy	- Identify critical & non critical business processes - Identify information assets needed for the execution of those processes - Analyze the risk of these assets (threats, vulnerabilities) - Compare current protection means **Support** - Risk analysis tool - Security checklists e.g SBA - Vulnerability scanner e.g Nmap	Assessment report such as: - Risk and Gap analysis reports - Technical report on vulnerabilities - Top management awareness - Understanding of how information security relates to business

Table 5-1 Template for Evaluation stage

A security requirement is driven by a risk assessment. The risk assessment will identify the main IT risks involved in operating the business in a secure manner. Once the risks are identified, controls to mitigate the risks can be selected.

The risk assessment will be supported by software tools like SBA, which is a software tool.

B. Formation stage

The goal of the formation stage is to design a technical and organizational infrastructure for information security that suits the business (table 5-2). Such an infrastructure is documented as an information security management system – often presented in the form of a security handbook for the bank. The written documents contain policies, procedures and guideline, with regards to how employees should handle information securely.

BRID	Inputs	Procedures	Out Puts
BR01	- All outputs from the evaluation stage - Cultural knowledge - Business- and IT knowledge - Counter measure / control / best practice knowledge - Current ISMS if any or any existing information security rules - Legal requirements such as: * Correspondent bank security agreement * Anti-money laundering and terrorist financing conventions -International commercial terms	- Identify external requirements on the ISMS - Identify internal requirements on the ISMS - Design and document counter measures - Write policy and procedures (ISMS) **Supports** - Information security standards - Electronic forum - ISMS templates if any	- Information security policy - Information security management system - counter measure design document - Partial Top Management awareness

Table 5-2 Template for Formation stage

C. Implementation stage

The goal of the implementation stage is to take the ISMS, including also the technical controls, from the design document to reality (table 5-3). This is the most difficult of all the stages, and it is also here that it will be evident if the other stages – the evaluation and formation stages – were carried out properly.

BRID	Inputs	Procedures	Out put
BR01	- All outputs from the formation stage - Profound technical knowledge	- Communicate the new rules throughout a bank -train employees to have security skills - Install and configure technical countermeasures - Market information security to create awareness **Supports** - brochure, bank's email - Intranet - Login message	- Signed information security agreements - Audit information -penetration testing report - Employees motivated to follow policies - Cost reductions and/or increased revenue

Table 5-3 Template for Implementation

The rules in the ISMS have to be communicated to relevant groups throughout the bank, employees have to be motivated and educated and trained in using new technical security controls and following the rules agreed to ISMS. Also, all the IT-related solutions have to be installed or (re-configured). Information security has to be marketed so that the bank accepts adherence to the rules laid out in the ISMS. This work can be aided by using a brochure or bank's email communicating the most important rules (e.g. "This is how you use the password") and explaining the most common technical controls. If all goes well, the employees will sign on and feel motivated to follow the rules in the ISMS. In that case, the result is that the bank will have reduced the cost from security breaches and in some cases even enabled new streams of revenue in the future.

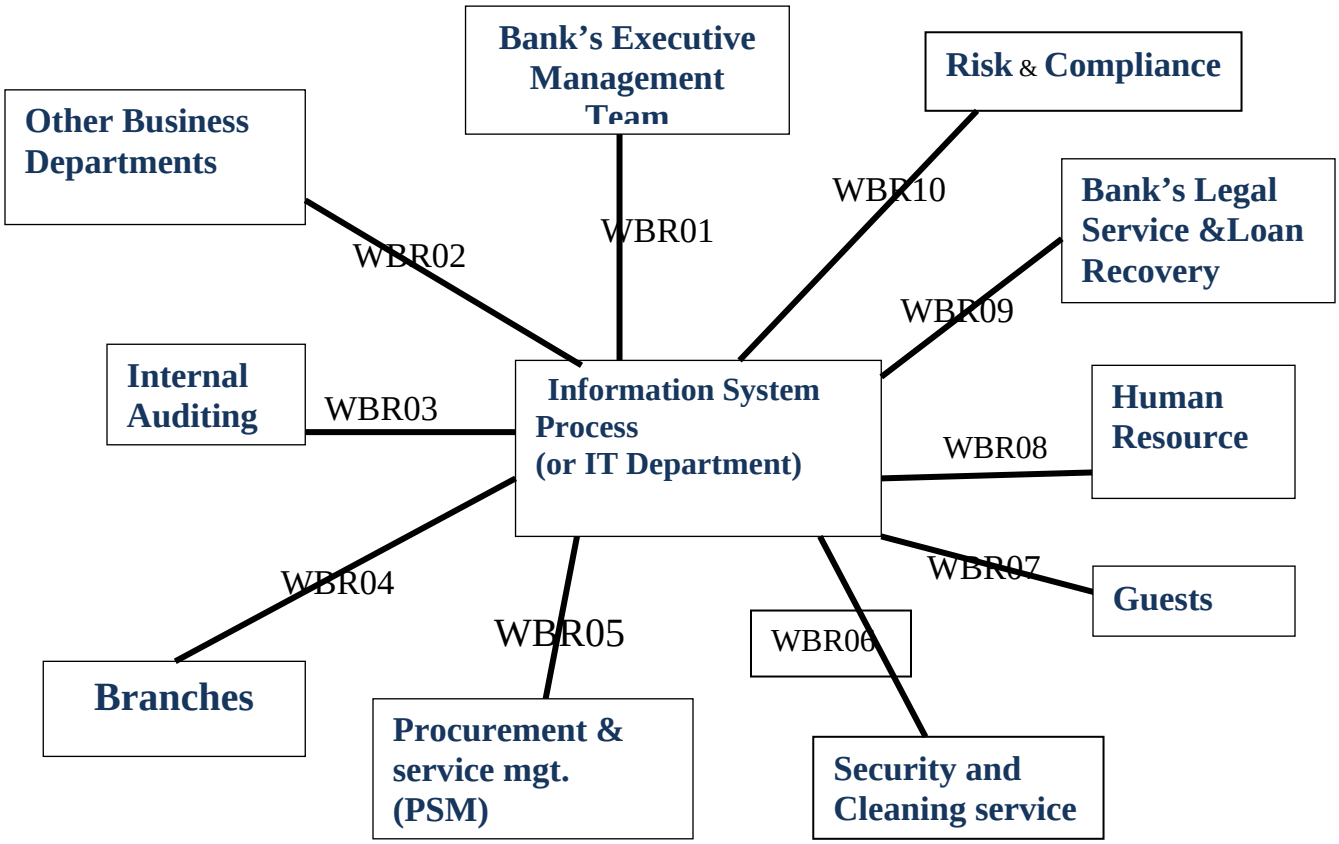
D. Feedback Mechanism

The feedback from all employees of the bank or any entity will be collected via email or forum discussion. The responsible body of the bank related to security will analyze and discuss with the top management about the pros and cons of the feedback and take action.

5.5.3 Within Ethio-Bank

For intra bank (within bank) also use the same process as inter entities by considering each process or department and branch as one entity and apply the same steps as above.

Information security management shall be accepted as an integral part of bank governance, in turn associates with IT /Information system management. Information security is concerned about the policies and procedures that define how a bank will direct and control the use of its technology and protect its information.



*WBR= Business Relationship Within Ethio-Bank

Figure5-4 internal entities relationship to Information System process

5.5.3.1 Description of Sstakeholders /Eentities within Ethio-bank

Even though the organizational structure of each bank somehow differs, the researcher tried to incorporate all stakeholders which have direct interaction with information system process owner in one or another way. These stakeholders should be participated in the development and implementation of ISMS process. These stakeholders are:

- ***Bank's Executive Management Team (BEMT)*:** it includes senior executive management members. BEMT is one of the key administrators of a financial institution. These chief managers perform long term planning, and regulatory compliance at a bank to ensure it meets the needs of customers and shareholders. To accomplish these tasks they should get bank's financial information from the system which is owned by Information System process /IT department.

- ***Information System Process:*** Ensures the smooth operation of the Information System process across the bank and Leads huge IT infrastructure investments and projects and more.
- ***The Risk & Compliance process:*** has a mandate to perform risk identification, assessment, control and monitoring of the bank's business risks.
- ***Legal Services and Loan Recovery Process:*** is responsible for timely and reliable legal services to processes of the bank. This process is also responsible for ensuring the provision of independent legal advice in the best interests of the bank and consistent with the bank's legal obligations.
- ***Other Business Departments:*** Provides a detailed record of the transaction coming in and going out of the business and prepares accounts as a basis for financial decisions. To accomplish these tasks they need to get bank's financial information from the system which is managed by IS department since it is the owner of the information system.
- ***Bank's Internal Audit Process:*** The Internal Audit Process (IAP) bears primary responsibility for audits. IAP conducts audits in accordance with the International Standards for the Professional Practice of Internal Auditing (Standards). In other words, Auditing department that inspect, analyze and rate the financial (or IT services) operations and practices of bank.
- ***Human Resource:*** Deals with all the recruitment, training, health and safety and pay negotiations with unions/workers of bank. And also it ensures the proper performance of the Human Resource Process across the bank.
- ***Procurement and Service Management:*** Buys all the supplies materials and goods required for bank and manage transport service. And it also performs asset inventory.
- ***Branches*****:** is part of the bank which has a mandate to accomplish bank's objective and mission at branch level. It also responsible for the branch system security.
- ***Guest*****:** a person who has limited access to bank's system based on the contractual agreement.
- ***Security and Cleaning Service:*** This has a mandate for assuring physical security of the bank and cleaning the server room/ datacenter and disaster recovery and the whole compound by large.
    - ***Janitor:*** Someone employed to clean and maintain a server room/ data center etc.
    - ***Security Guard:*** a person who has a responsibility and accountability for server room or datacenter external environment. On other words, A security guard or security officer is usually a privately and formally employed person who is paid to protect property, assets, or people. Often, security officers are uniformed act to protect property by maintaining a high visibility presence to deter illegal and inappropriate actions, observing (either directly, or by watching alarm systems or video) for signs of crime, fire or disorder; then taking action and reporting any incidents to his/her immediate boss. Moreover, they have a responsibility to check Visitors, Service Engineers, and Cleaning Staff when they enter and exit the data center. To achieve this objective a guard house

(also known as a watch house) should be built near to the data center which is used to house security personnel. This is required for both data center and disaster recovery sites. The security guard works 24x7x365.

5.5.3.2 Stakeholders' relationship with Information System Process

- *WBR01* is a Business Relationship (interaction) between Bank's executive management team to IS/IT Process
- *WBR02* is a Business Relationship (interaction) between other Business Departments
- to IS/IT Process
- *WBR03* is a Business Relationship (interaction) between Internal Auditing to IS/IT Process
- *WBR04* is a Business Relationship (interaction) between branches to IS/IT Process
- *WBR05* is a Business Relationship (interaction) between PSM to IS/IT Process
- *WBR06* is a Business Relationship (interaction) between Security and Cleaning service
- to IS/IT Process
- *WBR07* is a Business Relationship (interaction) between guests to IS/IT Process
- *WBR08* is a Business Relationship (interaction) between human resource to IS/IT Process
- *WBR09* is a Business Relationship (interaction) between Bank's Legal Service &Loan Recovery to IS/IT Process
- *WBR10* is a Business Relationship (interaction) between risk & compliance to IS/IT Process

A. Evaluation Stage

The goal of the evaluation stage is to assess the current information security situation of the Ethio-Bank (figure 5-4). This evaluation takes into account not only the administrative security issues, but also the technical (IT) security issues. Before any fruitful evaluation take place, ISMS development team of a bank needs to gather some information (table 5-4). That is, information gathering based on business objective and IT strategies of the bank. There should be pre-evaluation task.

Parameters that are considered in the template are:

- ***BRID***: Business Relationship Identification
- ***Description***: tells the involved entities in the given relationship or business process.
- ***Channel***: means of communication between any entities or departments within a bank. It determines mode of interaction among entities: viz, User to system, user to user

(Manual via messenger) or System to system (electronically like edge router to edge router).

- ***Inputs***: any documents like business objective, and channels. Inputs may differ in each stage.
- ***Procedures***: activities that are performed in each stage of ISMS process model.
- ***Outputs***: the result of each stage after processing the inputs.

BRID	Description	Channels	Inputs	Procedures	Out put
WBR04	A business relationship between IS and Branches	paper, email	- Business strategy - IT strategy - Process knowledge - Information assets -Public Financial institutions Agency's orders -Directives issued by the NBE -Policies and procedures of the bank -Directives issued by the bank -National Information Security Policy	- Identify critical & non critical business processes - Identify information assets needed for the execution of those processes - Analyze the security of these assets (threats, vulnerabilities) **Support** - Risk analysis tool e.g - Security checklists e.g SBA - Vulnerability scanner e.g Nmap	Assessment report such as: - Risk and Gap analysis reports - Technical report on vulnerabilities - Top management awareness - Understanding of how information security relates to business

Table 5-4 Template for intra-bank evaluation stage

B. Formation stage

The goal of the formation stage is to design a technical and organizational infrastructure for information security that suits the business (table 5-5). Such an infrastructure is documented as an information security management system – often presented in the form of a security handbook for the bank. The written documents contain policies, procedures and guideline, with regards to how employees should handle information securely.

BRID	Inputs	Procedures	Out Puts
WBR04	- All outputs from the evaluation stage - Cultural knowledge - Business- and IT knowledge - Countermeasure / control knowledge (efficiency, cost, etc.) - Best practice - Legal requirements - Current ISMS if any or any existing information security rules	- Identify internal requirements on the ISMS - Design and document technical countermeasures - Write policy and procedures (ISMS) **Supports** - Information security standards - Electronic forum - ISMS templates if any	- Information security policy - Information security management system - countermeasure design document - Partial organizational acceptance

Table 5-5 Template for intra-bank Formulation stage

C. Implementation stage

The goal of the implementation stage is to take the ISMS documents, including also the technical controls, from the design document to reality (table 5-6).

BRID	Inputs	Procedures	Out puts
WBR04	- All outputs from the formation stage - Profound technical knowledge	- Communicate the new rules throughout the organization - Educate employees to create security awareness - Install and configure technical countermeasures - Market information security **Supports** - brochure, bank's email - Intranet - Login message	- Signed information security agreements - Audit information -penetration testing report - Employees motivated to follow policies - Cost reductions and/or increased revenue

Table 5-6 Templates for intra-bank Implementation stage

5.6 ISM Framework Components- Counter measures' Categorization

It is noted that none of the frameworks /standards cover all information security management components; some of the framework such as PCIDSS security standard is very specific to operational level. Some other frameworks, such as ISO 27002 or the COBIT, also detailed technical practice security standards, which have the character of basic configuration and operation of IT systems.

Munirul , Zuraini , and Zailani (2011) state that although it is often speak of "best practice" in connection with data security, in practice there is no standard that completely regulates all of the aspects of information security and can fulfill the needs of individual banks to the same degree. The reasons why there cannot be universally correct information security, because of the significant differences between various economic operators, even within the same industry. Different banks have different sizes, financial strengths, organizational cultures, values, core competencies, visions, business strategies, business models, target customer segments, and also different risk policies. Thus, banks may have dissimilar ideas about the importance and value of information security for the achievement of particular business objectives and a correspondingly different willingness to pay for it.

Bank information security management should have its own place within the framework of bank governance, beside IT governance and risk management. The effectiveness of ISM depends on management's commitment and ability to clearly identify what makes existing business processes work properly and safely. Each bank should evaluate its own unique circumstances and environment to develop appropriate ISM policies and procedures. The required controls can be derived from the ISO/IEC 27002 standard, internal sources or any other sources such as COBIT, PCI DSS …etc.

Adapting to the information security controls from ISO/IEC 27k-series will provide the bank a solid base to build on. banks are free to choose any standard, however in order to have a common and solid foundation for ISM, the ISM policies, standards and procedures should at least consider the ISO/IEC 27002 control objectives in addition to controls added by the researchers in this paper.

Based on the literature review, questionnaires and interview findings 16 main control objects are identified. These components are further categorized into three major groups for easy of understanding such as Administrative, Physical & environmental, and Technical.

A. Administrative - Security Control Objects

- ***A1. Asset Management:*** To achieve and maintain appropriate protection of information assets.

- ***A2. Human Resource Security:*** To ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, ethical issues, fraud or misuse of facilities.
- ***A3. Information Security Incident Management:*** To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
- ***A4. Business Continuity Management:*** To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
- ***A5. Compliance:*** To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
- ***A6.Risk management:*** coordinated activities to direct and control an organization with regard to risk. It includes risk assessment, risk analysis, and risk evaluation.
- ***A7. Security Policy***: is a set of guidelines established to safeguard the network from attacks, both from inside and outside a bank. An information security policy must be developed which reflects bank's objectives, management support and commitment.
- ***A8. Organizing Information Security –*** Management must establish a framework to initiate and control the implementation of information security. Information security must extend to external parties.
- ***A9. Cultural analysis:*** To keep and understand the society where the business runs in.
- ***A10.Trust and ethical conduct:*** must be exercised in the bank to control human elements.

B. Physical and Environmental- Security Control Object

- ***P1. Physical and Environmental Security:*** To monitor and prevent unauthorized physical access, damage, and interference to the bank's premises and information resource.

C. Technical /Logical security- Security Control Objects

- ***T1. Communications and Operations Management*****:** To ensure the correct and secure operation of information processing facilities.
- ***T2. Access Control:*** To control read, add, update and delete access to information.
- ***T3. Information systems acquisition, development and maintenance:*** To ensure that security is an integral part of information systems.
- ***T4. Penetration testing:*** A penetration test is a method of evaluating the computer security of a computer system or network by simulating an attack from external threats and internal threats. Hack yourself before hacked by someone!
- ***T5. Information System Auditing:*** Defines audit policies to ensure the integrity of information and resources. This includes a process to investigate incidents, ensure conformance to security policies, and monitor user and system activity where appropriate.

All these 16 components or control objects, which are identified above, are summarized using organizational structure for easy understanding as shown in figure 5-5 below.

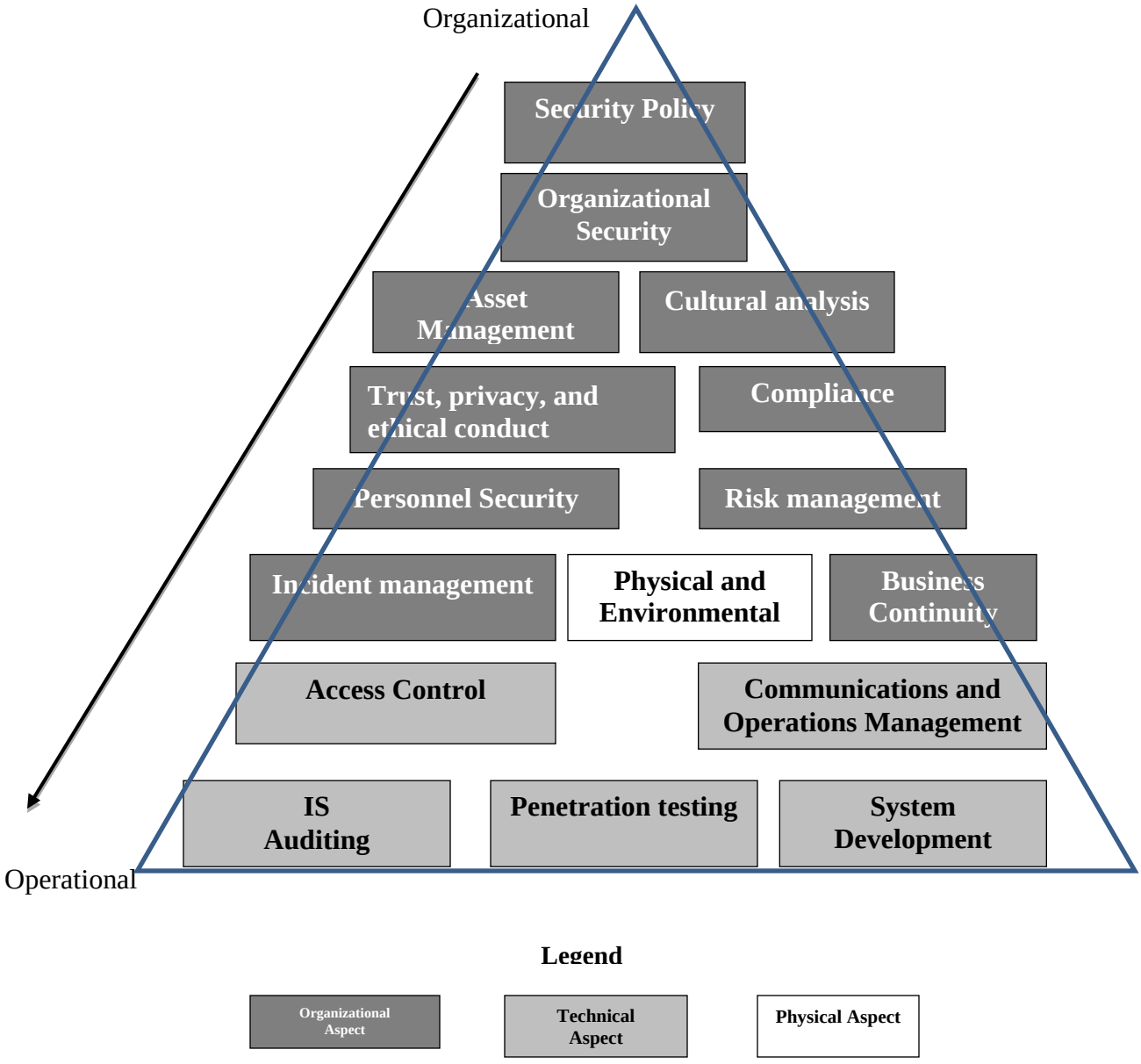


Figure 5-5 adapted from (Fredrik, 2005)

5.6.1 List of Recommended Information security Policies

When implementing the ISMS the combination of the technical, physical & environment, and administrative controls applicable to the bank's environment must be implemented.

A security policy is a living document, meaning that the document is never finished and is continuously updated as technology and employee requirements change. It acts as a bridge between management objectives and specific security requirements.

The information security policy is for everyone, including employees, contractors, suppliers, venders and customers who have access to the network. However, the security policy should treat each of these groups differently. Each group should only be shown the portion of the policy appropriate to their work and level of access to the network.

It is identified some of (around 21), not limited to, the components of compressive Information Security Policy of a bank that requires policy.

- ***Statement of authority and scope***- Defines who in bank sponsors the information security policy, and who is responsible for implementing it, and what areas are covered by the policy.
- ***Acceptable use policy (AUP)***-Defines the acceptable use of equipment and computing services, and the appropriate employee security measures to protect the bank's resources and proprietary information.
- ***Identification and authentication policy***-Defines which technologies the bank uses to ensure that only authorized personnel have access to its data.
- ***Internet access policy***-Defines what the bank will and will not tolerate with respect to the use of its Internet connectivity by employees and guests.
- ***Incident handling procedure***-Specifies who will respond to security incidents, and how incidents have to be handled.
- ***Account access request policy***-Formalizes the account and access request process within bank. Users and system administrators who bypass the standard processes for account and access requests can lead to legal action.
- ***IT Audit policy***-Defines audit policies to ensure the integrity of information and resources. This includes a process to investigate incidents, ensure conformance to security policies, and monitor user and system activity where appropriate.
- ***Information sensitivity policy***-Defines the requirements for identifying, classifying and securing information assets in a manner appropriate to its sensitivity level.
- ***Password policy***-Defines the standards for creating, protecting, and changing strong passwords.
- ***Risk assessment policy***-Defines the requirements and provides the authority for the "information security team" to identify, assess, and remediate risks to the information infrastructure associated with conducting business.
- ***Web server policy***-Defines the standards required by all web hosts.
- ***E-mail policy***-Defines content standards to prevent tarnishing the public image of the bank.

- ***Automatically forwarded e-mail policy***-Documents the policy restricting automatic e-mail forwarding to an external destination without prior approval from the appropriate manager or director.
- ***E-mail Retention Policy-*** is intended to help employees determine what information sent or received by email should be retained and for how long.
- ***Spam policy-***Defines how spam should be reported and treated.
- ***IT equipment Disposal Policy-*** defined procedures that ensure implementation of controls to address the reassignment or final disposition of hardware and electronic media.
- ***Wireless network security policy-*** defines the requirements for the secure implementation of wireless networking technology within bank. This policy applies to all wireless networking equipment, software and services used for official bank purposes.
- ***Mobile Banking Security policy-***defines security guidelines for mobile device banking applications (that is, banking from mobile phones and other mobile devices like iPhones with web access) and user requirements for enrolment to this service.
- ***Internet Banking Security Policy*** –defines the requirement of Internet banking users and enrolment process.
- ***Remote access policy-***Defines how remote users can use the remote access infrastructure of bank. Remote access policies may include:
    a. Defines the appropriate dial-in access and its use by authorized personnel.

    b. Defines the standards for connecting to the bank network from any host or network external to the bank.

- ***Data Center and Disaster Recovery Policy***

Some of the points which may include are:

- Physical Access Management (i.e. Door access control System). It will consider the following entities.
    - Data Center and Disaster recovery Tours / Visitors access
    - The scope of Vendors access
    - The scope of Ethio-Telecom and EEPCOA Service engineers access
    - Employees access
- Systems Monitoring
    - External (Network) System Monitoring/Intrusion Detection
    - Internal (Host) System Monitoring/Event Log Monitoring
- Environmental Controls system
    - CCTV/ IP Camera
    - Air conditioning units
    - indoor temperature and humidity management

    - Uninterruptible Power supply (UPS) – diesel back-up
    - Building Management System (BMS)
- Installation of new equipment and /or software
- Security guard and janitor (cleaning Issues) tasks

5.7 Evaluation of ISM Framework

Evaluation method of the ISM Framework may vary across researchers. Some of them are: providing theoretical demonstration as workshop for some group of domain experts, giving the document to practitioners for comment, and presents the framework for bank industry IT experts and collect valid comments.

In order to evaluate the framework by providing theoretical demonstration as workshop for some group of domain experts has money constraint for hall and related ceremony in addition to time constraint. Moreover, it is difficult and challenging to get domain experts in Ethiopian context.

An alternative evaluation method here would be a focus group of practitioners, as intended users. However, to search for practitioner opinions on likely use or adoption of the framework in the space of a few short hours would not be feasible. Providing sufficient knowledge of the proposed framework to draw out meaningful and thoughtful comments would require a large investment of time, not something that practitioners generally have in large amounts.

The student researcher has tried to prepared presentation for two banks' IT experts and collected valid comments. Some of the comments are stated under each parameter as shown below.

5.7.1 Evaluation parameters

- Is the literature review comprehensive and up-to-date?

  The literature review has reflected the current state of knowledge relevant to the study and gap is identified.
- Is the sample adequately described and reflective of population?

  Both the method of sampling and the size of the sample has stated clearly. So that, the reader can judge whether the sample is representative of the population or not.
- Is the selection of participants described and the sampling method identified?

  Sample banks are selected using lottery method where respondents are selected for their relevant knowledge or experience. Representativeness is not a criteria and purposive sampling is often used.
- How is the applicability of the proposed framework to Ethiopian banking industry?

It is applicable. However, it needs to be tested in real banking environment, refine again and again.

- Did the researcher achieve the initial objective(s)?

  Yes, general and specific objectives are well addressed in the research.

- Is the conclusion comprehensive?

  Conclusion has supported by the findings. The researcher has identified limitations to the study. And also the researcher has incorporated recommendations for further research.

CHAPTER SIX

CONCULUSION AND RECOMMENDATION

6.1 Conclusion

In today's technological and social environment, security is a very important part of a banking system. Business partners, suppliers, customers, and vendors require high information security from one to another, particularly when providing mutual network and information access. Banks ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances a bank's ability to preserve and increase market share.

Recognizing this fact, this research work was aimed at assessing the current Information Security Management (ISM) practices of banking sector, and to propose and develop ISM Framework. In this work, attempts were done to examine and compare the available ISM frameworks and best practices. This research combines ISO audit checklist and researcher's own experience to assess the information systems security practices in banking industry. Both qualitative and quantitative research approach were used. Data collections were done using questionnaire survey, document analysis, and interviews. To analyze the data SPSS tool is employed.

To develop the ISM framework scholars use different research approaches. Some scholars design their research in the following order: literature review ➔ Case study or Assessing ➔Propose a conceptual ISM Framework (Are, 2007). Others follow: literature review ➔ Propose ISM Framework ➔ reviewed by professionals and tested in the real banking environment (Munirul et al., 2011). However, the student researcher employed the following approach. Literature review ➔Assessment ➔Propose a conceptual ISM Framework➔evaluated by professionals.

Findings of the assessment based on the fact finding techniques employed, such as questionnaire survey, document analysis, and interviews, show that current information security management in the surveyed banks, generally lack of a formalized comprehensive framework-based Information security policy. This seemed to have an adverse effect on the effective management of information security in those banks.

The developed ISM Framework for banking system can be used as a starting point for banking sector to manage information security by developing guidelines and implementing controls to protect banking information assets from the threats identified in literature reviews.

The framework has two major components viz. Information security requirement identification mechanism which is the combination of ERM, and ISMS process model with supporting template and counter measures (controls). Further, there are 16 main ISM domains are identified in this research. And these further grouped under three categories viz. Administrative, Technical, and Physical & Environmental security.

This framework is an integration of all available framework components discussed and derived from literature review. The suggested framework is still a general approach to ISM program. It needs a detail policies and procedures formulation and comprehensive test in the real banking environment.

From the foregoing, it can be concluded that the developed framework based on the assessment results is valid and applicable in the banking industry to address the challenges related to information security.

6.2 Recommendation

The framework can be used as an initial effort for practitioners in the banking industry to manage their information security. The results from this research also imply further works for researchers and academicians.

6.2.1 For practitioners

- The framework can serve as a guide line for managers to formulate policies and procedures.
- The framework can serve as a guide line for developers to develop information security systems
- The framework can serve as a guide line for consultants
- It enables banks to have common ISM platform, so that experts can share skills and knowledge easily via body of knowledge.

6.2.2 Areas for Further Research

Some aspects of ISM that are beyond the scope of this thesis research are recommended for future research. These are:

- Look into how to measure security management effectiveness in the context of bank security strategy, and develop metrics to be used against security goals, and objectives.
- Determine the impact level of trust, ethical conduct, and culture on the process of ISMS development and implementation in banking sector.
- How do banks develop a security culture?
- Enhancing the same research by considering all branches of banks.

- Further detail research will be made on the identified areas that require policies and procedures
- Evaluating the proposed ISMF practically via comprehensive test in the real banking environment.

References

- Abiy, W., and Lemma, L. (2012). Information Security Culture in the Banking Sector. Ethiopia. 5th ICT 2012 Ethiopia Conference. Venue: UN ECA, Addis Ababa, Ethiopia
- Anene, L.N. (2007). A Framework and Methodology for Information Security Management
- Anene, L. N., & Annette, L. S. (2007). An Architectural and Process Model Approach to Information Security Management. Lawrence Technological University.
- Are, N. (2007). Managing information security in organizations. A CASE study. Master thesis in information systems.
- Anon (2009). International Journal of Electronic Security and Digital Forensics [Online] 2(3), P. 306 – 321 Retrieved from: http://www.inderscience.metapress.com/openurl.asp?genre=article&issn=1751-911X&volume=2&issue=3&spage=306. Accessed Date: 12 Sep 2012 9:31 AM
- Benjamin, T. (2004). Information Security Technologies. The George Washington University.
- BSI-standard 100-1 (2008). Information Security Management System (ISMS)
- C.R.Kothari (2007).Research methodology: Methods &Techniques. 2nd ed. India: New Age International (P) Ltd., Publishers.
- Dean, C. V., Achilles, A. A., & Hubert, S. F. (2008). Integrating Qualitative and Quantitative Methods for Organizational Diagnosis. Possible Priming Effects? Auburn University, Alabama. Journal of Mixed Methods Research, Volume 2 number1, Sage Publications
- Dancho, D. (2003). Building and Implementing a Successful Information Security Policy [online]. Available at: http://www.windowsecurity.com . Internet Software Marketing Ltd. Accessed date: 14 April 2011
- Edward, E. (2011). The Importance of Managing Information Security from a CEO Perspective: [Newsletter] Available at: http://www.secureworks.com/research/newsletter/2003/07. Accessed Date: 12 April 2012
- Endale, M. (2012). ISO27k vis-à-vis PCI DSS. What comes first ISO or PICDSS?
- Federal Democratic Republic of Ethiopia (FDRE, 2011). National Information Security policy. Published in September 2011.

- Fiona, P. (2007). Certifying Information Security Management Systems.
- Fredrik. J. B. (2005). Discovering information Security Management. Stockholm: Department of Computer and Systems Sciences Stockholm University & Royal Institute of Technology.
- Gary, H. (2012). What comes first ISO or PICDSS? Retrieved from: https://groups.google.com/forum/?fromgroups=#!topic/iso27001security/ytJ9UvUa2q0. Accessed Date: On Tuesday, Nov 13, 2012 9:37:18 AM
- George, S., Dawn, C., Andrew, M., Randall, T., Timothy, J. S., & Lori, F. (2012). Common Sense Guide to Mitigating Insider Threats 4th Edition. Software Engineering Institutes.
- Heru, S., Mohammad, N. A., & Yong, C.T. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05
- Institute for Development and Research in Banking Technology (IDRBT, 2011). IT Governance Series: Information Security Governance for the Indian Banking Sector, Version 1.0, an IDRBT Publication.
- ISO/IEC 27001-2 (2005). Information technology – Security techniques – Information security management systems – Requirements.
- ISACA (1996). Control Objectives for Information and related Technology (COBIT). Retrieved from: http://www.the281group.com/index.php/control-objectives-for-information-and-related-technology-cobit. Accessed Date: 26 January 2013.
- Jimmy (2012). COBIT in Relation to Other International Standards. Retrieved from: http://www. COBIT-in-Relation-to-Other-International-Standards.aspx.htm. accessed date: 13 Dec 2012.
- Kei, H. (2004). Japanese Information Security Status - Environment and Policies: Security Center, Information-technology Promotion Agency, Japan.
- Matthias, M., Deborah, B., & Birgit, M. (2012) Mixed Methods: Combining Expert Interviews, Cross-Impact Analysis and Scenario Development .University of Canberra, Australia. Electronic Journal of Business Research Methods Volume 10
- Mohammed, A., & Karen, N. (2009). Proceedings of the 7th Australian Information Security Management Conference: A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context.

- Michael, E. W.(2003). Communications of the ACM. Enemy at the Gate: Threats to Information Security.
- Michael, L. (2007). Information security architecture Building security into organization.
- Mohan, K., & ISO27k Implementers' forum (2012). The User Awareness Training Of ISMS ISO/IEC 27001:2005
- Munirul, U., Zuraini, B., I., & Zailani, M. S. (2011). A Framework for the Governance of Information Security in Banking System.
- National Institute of Standards and Technology (NIST, 2012). Risk assessment framework
- Office of the Chief Information Officer (2012). GOVERNMENT FRAMEWORK ON CYBER SECURITY. Information Security Management Framework, Government of South Australia.
- Patrick, D. G. (2011). Managing Information Security Risk: Organization, Mission, and Information System View: U.S. Special Publication 800-39
- Philippa, A. L. (2004). Responsibilities of Management, Information Technology Personnel and the Consumer: SANS Institute InfoSec Reading Room. GSEC Practical version 1.4b.
- Tomonari, T.(2008). ICTs for Development in Ethiopia A Case of the SchoolNet Project. A dissertation submitted to the University of Manchester for the degree of MSc in the Faculty of Humanities.
- Victorian Managed Insurance Authority (VMIA, 2010). Risk Management; Developing & Implementing a Risk Management Framework
- Yigezu, B. J. (2011). Information System Security Audit Readiness. Case study: Ethiopian Government Organizations.
- Yegidis, B. L., & Weinbach, R. W. (1996). Research Methods for Social Workers, 2nd Edition, Allyn and Bacon, Boston, Massachusetts

APPENDIX A: Questionnaire

Instruction: Please put a "✓"sign in the square bracket [ ] for each item. You can also write your opinion or justification for open ended question.

Part I. Respondent Information

- Name of the Bank----------
- Job Title of the Respondent----------

Part II. Physical and Environmental Security

1. Physical security is critical to achieving confidentiality and availability goals of mission critical facilities like server rooms/ data center. What kind of security enforcement is/are used to protect it.
   a. alternate power source like generator[ ] Yes [ ] No
   b. air conditioning [ ] Yes [ ] No
   c. water leakage management and Fire suppression systems[ ] Yes [ ] No
   d. Fences and /or Human security guards[ ] Yes [ ] No
   e. Door Access system (Biometrics or card or PIN), conventional key and CCTV camera [ ] Yes [ ] No
2. Are visitors and contractors supervised when they visiting your servers room? [ ] Yes [ ] No
3. Does authorization and checking occur on equipment entering or leaving your site? [ ]Yes [ ] No
4. Does Sensitive data and licensed software removed from data-storage equipment prior to disposal? [ ] Yes [ ] N o

Part III. Technical/Operational security

5. Have you used an internal firewall which is between intranet and DMZ (demilitarized zone)? [ ] Yes [ ] No
6. Have you used an external firewall which is between the DMZ (demilitarized zone) and internet or outside world? [ ] Yes [ ] No
7. If the answer under #5 & # 6 is Yes, have you used different vendors firewall for the internal and external perimeter firewall? [ ] Yes [ ] No
8. Does your bank implement internetwork management system like Cisco works or Cisco Access Control server or Cisco Security Management Systems? [ ] Yes [ ] No
9. Does your bank implement wireless network? [ ] Yes [ ] No
10. If the answer of # 9 is Yes, Have you used authentication and encryption technologies like WEP or WPA or any other for Wireless LAN network security? [ ] Yes [ ] No
11. Is antivirus installed and regularly updated on the computers that exist in your Bank? [ ] Yes [ ] No
12. Is all the traffic originating from un-trusted network in to the bank flittered by firewall and web security for malicious? [ ] Yes [ ] No
13. Do you have any documented operating procedures such as for back-up, equipment maintenance, etc.? [ ] Yes [ ] No
14. Is back up of essential information taken regularly? [ ] Yes [ ] No
    If yes, how often you take back up? ----------
15. Does Internet line and data line (for example CORE banking) is separated? [ ] Yes [ ] No
16. Does the bank have patch management procedure to known vulnerabilities? [ ] Yes [ ] No
17. Are system logs monitored and logged? [ ] Yes [ ] No

18. When a new system (such as Firewalls, Routers, Switches etc) is installed on the network what kind of steps that should be taken?
    a. Default usernames and passwords will change immediately. [ ] Yes [ ] No
    b. Access to system resources should be restricted to only the individuals that are authorized to use those resources. [ ] Yes [ ] No
    c. Any unnecessary protocol and services will disable /close. [ ] Yes [ ] No
19. Is there formal defined user access control policy document for granting access to multi-user information systems and services? [ ] Yes [ ] No
20. Does the bank has formal user registration and de-registration procedure document? [ ] Yes [ ] No
21. Do you have any procedures and a process to review user access rights at regular intervals? [ ] Yes [ ] No
    If yes, how often you conduct the review? ----------
22. Does the bank has password guidelines (about its complexity, change period, password reset, access attempt and lockout ...etc.) for the users in selecting and maintaining of password [ ] Yes [ ] No
23. Do you have any authentication mechanism for challenging external connections? [ ] Yes [ ] No
24. If your answer to question # 23 is yes, which of the following mechanisms are used?
    a. Cryptography based technique (Encryption &Digital signature) [ ] Yes [ ] No
    b. hardware or software tokens [ ] Yes [ ] No
25. Are security requirements derived from a business risk assessment? [ ] Yes [ ] No
26. Is there a culture of conducting security requirement study before systems development and test its security related issue in your bank? [ ] Yes [ ] No

Part .IV Administrative - Security Policy and Standards

27. Do you have Security policy document to ensure the security of your Bank's information system?
    [ ] Yes [ ] No
    If your answer is no, what is the reason and your future plan with this regard?

    ----
28. If your answer to question # 27 is yes, to what extent it is implemented?
    [ ] Implemented [ ] in plan stage for implementation [ ] not implemented
29. How often you update the policy document?
    [ ] Annually [ ] every two year[ ] Never updated [ ] others, please specify----------
30. Does the information security policy consider all stakeholders such as employees, contractors, suppliers/venders, service providers, and customers who have access to the bank's network? [ ] Yes [ ] No
31. What standards or framework you follow in the process of implementation of your Information systems security? [ ] ISO/IEC 27002:2005 [ ] Industry Standards [ ] Unknown
    [ ] Others, please Specify----------
32. If you have information security policy does the following stakeholders such as Security specialists, technical staff, administrator (or HR), legal advisor, internal Auditor, Risk and compliance, and Top management were involved in its development? [ ] Yes [ ] No
33. Does the bank performing risk assessment to identify its security requirements prior to select best practices or controls? [ ] Yes [ ] No
34. Do you think that lack of experienced staff on international standards, lack of **local** Information Security Management Framework/standard, and budget are problems that ***hindered*** the implementation of Information Security Management System *in your bank?* [ ] Yes [ ] No
35. Does your bank have a dedicated individual (or individuals) with responsibility for information security?
    [ ] Yes [ ] No
36. How do you rate the management support in Information System security assurance process?
    [ ] Low [ ] Medium [ ] High

37. Is there management authorization process in place for any new information processing facility including all new facilities such as hardware and software? [ ] Yes [ ] No
38. Does the bank has a yearly budget for staff information Security awareness program and technical training? [ ] Yes [ ] No
39. Do you think that separating Information security team from other IT staffs structurally under IT department is advantageous from security assurance perspective? [ ] Yes [ ]NO
    If the answer is no, why? ----------
40. Are duties and areas of responsibility separated in order to reduce opportunities for unauthorized modification or misuse of information or services? [ ] Yes [ ] No
41. Is there formal contract contain, or refer to, all the security requirements to ensure compliance with the Bank's security policies and standards? [ ] Yes [ ] No
42. Have you ever audited your information systems security in a regular base? [ ] Yes [ ] No
43. Have you outsourcing the IT Systems Security audit to third party? [ ] Yes [ ] No
44. Are risks from third party access identified and appropriate security controls implemented? [ ] Yes [ ] No
45. Does the bank conduct formal risk management activity before developing an Information security policy? [ ] Yes [ ] No
46. Does the bank has defined Information asset inventory and classification scheme or guideline in place; which will assist in determining how information is to be handled and protected? [ ] Yes [ ] No
47. Does employees' written job description include responsibility for information security? [ ] Yes [ ] No
48. Does the bank invite employees to be involved in the development of information security policies in order to encourage a sense of ownership? [ ] Yes [ ] No
49. Are employees sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment? [ ] Yes [ ] No
50. How often all employees of the bank and third party users receive appropriate Information Security awareness and regular updates on banks policies and procedures?
    [ ] Once a year [ ] Twice a year [ ] don't conduct training and updates
    [ ] Other, please specify----------
51. How do you rate technical staffs' awareness about emerging technologies and related control issues? [ ] Low [ ] medium [ ] high
52. Do you have written incident Management and formal reporting procedure to handle security incidents? [ ] Yes [ ] No
53. Does the bank have an approved business Continuity plan? [ ] Yes [ ] No
54. Does the bank have disaster recovery plan? [ ] Yes [ ] No
55. Does the bank perform periodical penetration testing of their infrastructure? [ ] Yes [ ] No

If you have any suggestion which is/are related to the research topic, please state here: ---

---

APPENDIX B: Interview Questions

1. If you have developed ISMS in your bank, what kind of standard or framework the bank is employed in the process of ISMS development? If not developed ISMS, what are the reasons?
2. What is/are the drawback(s) and strength of the standard that you have employed in ISMS development?
3. What are the negative (impending) elements of ISMS development and implementation process? And what are the critical success factors for a successful development and implementation of ISMS?
4. How the bank identifies its security requirements prior to select best practices or controls? Does it use a model? If so, what are the drawbacks and strengths of the model that you have employed for security requirement identification?
5. What kind of IT risk management methodology you have used?
6. What is your opinion about the pros and cons of separating Information security management team from other IT staffs structurally in IT department?

APPENDIX C: Finding Summery of Questionnaire

Security Categories	*Security Domain*	*NO.*	*Issues addressed in each security domains(Items lists)*	*responding value in % (Yes)*
Physical & Environmental	*Physical & Environmental*	*1*	*Physical security is critical to achieving confidentiality and availability goals of mission critical facilities like server rooms/ data center. What kind of security enforcement is/are used to protect it.*	
			a. alternate power source like generator	*100%*
			b. air conditioning	*100%*
			c. water leakage management and Fire suppression systems	*80%*
			d. Fences and /or Human security guards	*100%*
			e. Door Access system (Biometrics or card or PIN), conventional key and CCTV camera	*80%*
		2	*Are visitors and contractors supervised when they visiting your servers room?*	*60%*
		3	*Does authorization and checking occur on equipment entering or leaving your site?*	*60%*
		4	*Does Sensitive data and licensed software removed from data-storage equipment prior to disposal?*	*40%*
Technical	*communication & Operation*	*5*	*Have you used an internal firewall which is between intranet and DMZ (demilitarized zone)?*	*60%*
		6	*Have you used an external firewall which is between the DMZ (demilitarized zone) and internet or outside world?*	*80%*
		7	*If the answer under #5 & #6 is Yes, have you used different vendors firewall for the internal and external perimeter firewall?*	*60%*
		8	*Does your bank implement internetwork management system like cisco works or cisco Access Control server or Cisco Security Management Systems?*	*60%*
		9	*Does your organization implement wireless network?*	*80%*
		10	*If the answer is Yes, Have you used authentication and encryption technologies like WEP for Wireless LAN network security?*	*80%*
		11	*Is antivirus installed and regularly updated on the computers that exist in your Bank?*	*100%*
		12	*Is all the traffic originating from un-trusted network in to the bank flittered by firewall and web security for malicious?*	*80%*

		13	*Do you have any documented operating procedures such as for back-up, equipment maintenance, etc.?*	*40%*
		14	*Is back up of essential information taken regularly*	*100%*
		15	*Does Internet line and data line (for example CORE banking) is separated?*	*100%*
		16	*Does the bank have patch management procedure to known vulnerabilities?*	*40%*
		17	*Are system logs monitored and logged?*	*40%*
	Access Control	*18*	*When a new system (such as Firewalls, Routers, Switches etc) is installed on the network what kind of steps that should be taken?*	*100%*
			a. Default usernames and passwords will change immediately.	
			b. Access to system resources should be restricted to only the individuals that are authorized to use those resources.	*80%*
			c. Any unnecessary protocol and services will disable.	*60%*
		19	*Is there formal defined user access control policy document for granting access to multi-user information systems and services?*	*40%*
		20	*Does the bank has formal user registration and de-registration procedure document?*	*80%*
		21	*Do you have any procedures and a process to review user access rights at regular intervals?*	*20%*
		22	*Does the bank has password guidelines (about its complexity, change period, password reset, access attempt and lockout ...etc.) for the users in selecting and maintaining of password*	*80%*
		23	*Do you have any authentication mechanism for challenging external connections?*	*60%*
		24	*If your answer to question # 23 is yes, which of the following mechanisms are used?*	*60%*
			a. Cryptography based technique (Encryption &Digital signature)	
			b. hardware or software tokens	*40%*
	System development	*25*	*Are security requirements derived from a business risk assessment?*	*40%*
		26	*Is there a culture of conducting security requirement study before systems development and test its security related issue in your bank?*	*60%*
Administrative	*Security policy*	*27*	*Do you have Security policy document to ensure the security of your Bank's information system?*	*80% Yes*
		28	*If your answer to question # 27 is yes, to what extent it is implemented?*	*40% not implemented, 40% in plan stage, 20% implemented*
		29	*How often you update the policy document?*	*40% every 2 years, 20% never updated, 40% others(as required)*

		30	*What standards or framework you follow in the process of implementation of your Information systems security?*	*40% ISO/ICE27002:2005, 20% industry standard, 40% others(NBE policy, National Information security policy)*
		31	*Does the information security policy consider all stakeholders such as employees, contractors, suppliers/venders, service providers, and customers who have access to the bank's network?*	*60%*
		32	*If you have information security policy does the following stakeholders such as Security specialists, technical staff, administrator (or HR), legal advisor, internal Auditor, Risk and compliance, and Top management were involved in its development?*	*20%*
		33	*Does the bank performing risk assessment to identify its security requirements prior to select best practices or controls?*	*40%*
	Organizational Security	*34*	*Do you think that lack of experienced staff on international standards, lack of local Information Security Management Framework/standard, and budget are problems that hindered the implementation of Information Security Management System in your bank?*	*100%*
		35	*Does your bank have a dedicated individual (or individuals) with responsibility for information security?*	*40%*
		36	*How do you rate the management support in Information System security assurance process?*	*20% low,40% medium, And 40% high*
		37	*Is there management authorization process in place for any new information processing facility including all new facilities such as hardware and software?*	*100%*
		38	*Does the bank has a yearly budget for staff information Security awareness program and technical training ?*	*40%*
		39	*Do you think that separating Information security team from other IT staffs structurally under IT department is advantageous from security assurance perspective?*	*100%*
		40	*Are duties and areas of responsibility separated in order to reduce opportunities for unauthorized modification or misuse of information or services?*	*40%*
		41	*Is there formal contract contain, or refer to, all the security requirements to ensure compliance with the Bank's security policies and standards?*	*40%*
	compliance	*42*	*Have you ever audited your information systems security in a regular base?*	*40%*
		43	*Have you outsourcing the IT Systems Security audit to third party?*	*20%*
	Risk management	*44*	*Are risks from third party access identified and appropriate security controls implemented?*	*40%*
		45	*Does the bank conduct formal risk management activity before developing an Information security policy?*	*40%*

	Asset management	***46***	***Does the bank have defined Information asset inventory and classification scheme or guideline in place; which will assist in determining how information is to be handled and protected?***	***80%***
	Personnel Security	***47***	***Does employees' written job description include responsibility for information security?***	***20%***
		48	***Does the bank invite employees to be involved in the development of information security policies in order to encourage a sense of ownership?***	***20%***
		49	***Are employees sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment?***	***40%***
		50	***How often all employees of the bank and third party users receive appropriate Information Security awareness and regular updates on banks policies and procedures?***	***40% don't conduct, 40% once a year, 20% twice a year***
		51	***How do you rate technical staffs' awareness about emerging technologies and related control issues?***	***40% low,40% Medium, 20% high***
	incident magt	***52***	***Do you have written incident Management and formal reporting procedure to handle security incidents?***	***40%***
	Business continuity	***53***	***Does the bank have an approved business Continuity plan?***	***60%***
		54	***Does the bank has tested disaster recovery plan?***	***60%***
	penetration testing	***55***	***Does the bank has periodical penetration testing culture of their infrastructure?***	***40%***

APPENDIX D: Summary of Response by Banks

Security Categories	Security Domain	Question NO.	Issues addressed in each security domains(Items lists)	Response by banks under study(banks are represented from 1 – 5) and Y=Yes, N=No				
				1	2	3	4	5
Physical & Environmental	Physical & Environmental	1	Physical security is critical to achieving confidentiality and availability goals of mission critical facilities like server rooms/ data center. What kind of security enforcement is/are used to protect it.	Y	Y	Y	Y	Y
			a. alternate power source like generator					
			b. air conditioning	Y	Y	Y	Y	Y
			c. water leakage management and Fire suppression systems	Y	Y	Y	N	Y
			d. Fences and /or Human security guards	Y	Y	Y	Y	Y
			e. Door Access system (Biometrics or card or PIN), conventional key and CCTV camera	Y	Y	Y	N	Y
		2	Are visitors and contractors supervised when they visiting your servers room?	Y	Y	Y	N	N
		3	Does authorization and checking occur on equipment entering or leaving your site?	Y	Y	Y	N	N
		4	Does Sensitive data and licensed software removed from data-storage equipment prior to disposal?	N	Y	Y	N	N
Technical	communication & Operation	5	Have you used an internal firewall which is between intranet and DMZ (demilitarized zone)?	Y	Y	Y	N	N
		6	Have you used an external firewall which is between the DMZ (demilitarized zone) and internet or outside world?	Y	Y	Y	N	Y
		7	If the answer under #5 & #6 is Yes, have you used different vendors firewall for the internal and external perimeter firewall?	Y	Y	N	N	Y
		8	Does your bank implement internetwork management system like cisco works or cisco Access Control server or Cisco Security Management Systems?	Y	Y	Y	N	N

	9	*Does your organization implement wireless network?*	*Y*	*Y*	*Y*	*Y*	*N*
	10	*If the answer is Yes, Have you used authentication and encryption technologies like WEP or WPA for Wireless LAN network security?*	*Y*	*Y*	*Y*	*Y*	*N*
	11	*Is antivirus installed and regularly updated on the computers that exist in your Bank?*	*Y*	*Y*	*Y*	*Y*	*Y*
	12	*Is all the traffic originating from un-trusted network in to the bank flittered by firewall and web security for malicious?*	*Y*	*Y*	*Y*	*N*	*Y*
	13	*Do you have any documented operating procedures such as for back-up, equipment maintenance, etc.?*	*N*	*Y*	*Y*	*N*	*N*
	14	*Is back up of essential information taken regularly*	*Y*	*Y*	*Y*	*Y*	*Y*
	15	*Does Internet line and data line (for example CORE banking) is separated?*	*Y*	*Y*	*Y*	*Y*	*Y*
	16	*Does the bank have patch management procedure to known vulnerabilities?*	*N*	*N*	*Y*	*N*	*Y*
	17	*Are system logs monitored and logged?*	*N*	*Y*	*Y*	*N*	*N*
Access Control	*18*	*When a new system (such as Firewalls, Routers, Switches etc) is installed on the network what kind of steps that should be taken?*	*Y*	*Y*	*Y*	*Y*	*Y*
		a. Default usernames and passwords will change immediately.					
		b. Access to system resources should be restricted to only the individuals that are authorized to use those resources.	*Y*	*Y*	*Y*	*N*	*Y*
		c. Any unnecessary protocol and services will disable.	*Y*	*Y*	*Y*	*N*	*N*
	19	*Is there formal defined user access control policy document for granting access to multi-user information systems and services?*	*N*	*Y*	*N*	*N*	*Y*
	20	*Does the bank has formal user registration and de-registration procedure document?*	*N*	*Y*	*Y*	*Y*	*Y*
	21	*Do you have any procedures and a process to review user access rights at regular intervals?*	*N*	*Y*	*N*	*N*	*N*

		22	Does the bank has password guidelines (about its complexity, change period, password reset, access attempt and lockout ...etc.) for the users in selecting and maintaining of password	Y	Y	Y	N	Y
		23	Do you have any authentication mechanism for challenging external connections?	Y	N	Y	N	Y
		24	If your answer to question # 23 is yes, which of the following mechanisms are used?	Y	Y	Y	N	N
			a. Cryptography based technique (Encryption &Digital signature)					
			b. hardware or software tokens	N	Y	Y	N	N
	System development	25	Are security requirements derived from a business risk assessment?	N	N	Y	N	Y
		26	Is there a culture of conducting security requirement study before systems development and test its security related issue in your bank?	N	Y	Y	N	Y
Administrative	Security policy	27	Do you have Security policy document to ensure the security of your Bank's information system?	Y	Y	Y	N	Y
		28	If your answer to question # 27 is yes, to what extent it is implemented?	Not Implemented	Not Implemented	Implemented	In plan stage of Implementation	In plan stage of Implementation
		29	How often you update the policy document?	others	others	Every 2 years	Never updated	Every 2 years
		30	What standards or framework you follow in the process of implementation of your Information systems security?	Industry standard	ISO/ICE27002: 2005	ISO/ICE27002: 2005	others	others
		31	Does the information security policy consider all stakeholders such as employees, contractors, suppliers/venders, service providers, and customers who have access to the bank's network?	Y	Y	Y	N	N

		32	*If you have information security policy does the following stakeholders such as Security specialists, technical staff, administrator (or HR), legal advisor, internal Auditor, Risk and compliance, and Top management were involved in its development?*	*N*	*N*	*Y*	*N*	*N*
		33	*Does the bank performing risk assessment to identify its security requirements prior to select best practices or controls?*	*N*	*Y*	*Y*	*N*	*N*
	Organizational Security	*34*	*Do you think that lack of experienced staff on international standards, lack of local Information Security Management Framework/standard, and budget are problems that hindered the implementation of Information Security Management System in your bank?*	*Y*	*Y*	*Y*	*Y*	*Y*
		35	*Does your bank have a dedicated individual (or individuals) with responsibility for information security?*	*N*	*Y*	*Y*	*N*	*N*
		36	*How do you rate the management support in Information System security assurance process?*	*M*	*H*	*H*	*L*	*M*
		37	*Is there management authorization process in place for any new information processing facility including all new facilities such as hardware and software?*	*Y*	*Y*	*Y*	*Y*	*Y*
		38	*Does the bank has a yearly budget for staff information Security awareness program and technical training ?*	*N*	*Y*	*Y*	*N*	*N*
		39	*Do you think that separating Information security team from other IT staffs structurally under IT department is advantageous from security assurance perspective?*	*Y*	*Y*	*Y*	*Y*	*Y*
		40	*Are duties and areas of responsibility separated in order to reduce opportunities for unauthorized modification or misuse of information or services?*	*N*	*Y*	*Y*	*N*	*N*
		41	*Is there formal contract contain, or refer to, all the security requirements to ensure compliance with the Bank's security policies and standards?*	*Y*	*N*	*N*	*N*	*Y*
	compliance	*42*	*Have you ever audited your information systems security in a regular base?*	*N*	*Y*	*Y*	*N*	*N*
		43	*Have you outsourcing the IT Systems Security audit to third party?*	*N*	*Y*	*N*	*N*	*N*
	Risk managem	*44*	*Are risks from third party access identified and appropriate security controls implemented?*	*N*	*N*	*Y*	*N*	*Y*

	ent	*45*	*Does the bank conduct formal risk management activity before developing an Information security policy?*	*N*	*Y*	*Y*	*Y*	*N*
	Asset managem ent	*46*	*Does the bank have defined Information asset inventory and classification scheme or guideline in place; which will assist in determining how information is to be handled and protected?*	*N*	*N*	*Y*	*N*	*N*
	Personnel Security	*47*	*Does employees' written job description include responsibility for information security?*	*N*	*N*	*Y*	*N*	*N*
		48	*Does the bank invite employees to be involved in the development of information security policies in order to encourage a sense of ownership?*	*N*	*Y*	*N*	*N*	*N*
		49	*Are employees sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment?*	*Y*	*N*	*N*	*N*	*Y*
		50	*How often all employees of the bank and third party users receive appropriate Information Security awareness and regular updates on banks policies and procedures?*	*Don't conduct*	*Once year*	*Don't conduct*	*Twice a year*	*Once year*
		51	*How do you rate technical staffs' awareness about emerging technologies and related control issues?*	*M*	*H*	*M*	*L*	*L*
	incident magt	*52*	*Do you have written incident Management and formal reporting procedure to handle security incidents?*	*N*	*N*	*Y*	*N*	*Y*
	Business continuity	*53*	*Does the bank have an approved business Continuity plan?*	*N*	*N*	*Y*	*Y*	*Y*
		54	*Does the bank has tested disaster recovery plan?*	*N*	*N*	*Y*	*Y*	*Y*
	penetratio n testing	*55*	*Does the bank has periodical penetration testing culture of their infrastructure?*	*N*	*Y*	*Y*	*N*	*N*