ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATE STUDIES

Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia

By

Tesfaye Asfaw Getahun

Advisor: Asrat Mulatu (PhD)

July10, 2018

Addis Ababa, Ethiopia

Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia

By

Tesfaye Asfaw Getahun

A Thesis Submitted to the Faculty of Informatics, St. Mary's University, in Partial fulfillment of the requirements for the Degree of Master of Science in Computer Science.

July10, 2018

Addis Ababa, Ethiopia

ST. MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia

By

Tesfaye Asfaw Getahun

APPROVED BY BOARD OF EXAMINERS

Asrat Mulatu (PhD)	_____
Dean, Faculty of Informatics	**Signature**
Asrat Mulatu (PhD)	_____
Advisor	**Signature**
Temitime_Assefa(PhD)	_____
External Examiner	**Signature**
Getahun Semeon (PhD)	_____
Internal Examiner	**Signature**

July 10, 2018

Addis Ababa, Ethiopia

Acknowledgments

First and for most I would like to thank the Almighty GOD for his unending helps and blessings to complete my thesis, without his blessings and support I wouldn't have been write a single word. Next I would like to express my special appreciation and thanks to my advisor, Asrat Mulatu (PhD) for the guidance and support in my research work. I would like to extend my appreciation to my family members especially my beloved wife W/o Yeshashework Abebe for her kind support and encouragement, and pray for the success of my work. And I am also grateful thanks to my best friend shimelies Tamiru for the support and encouragement. My thanks also extend to Ato Dawit from abysinya bank, W/o Yeshiwork from CBE and Ato Samson Tesfaye from Dashen Bank for their support during the data collection process. I am also very thankful to all staff members of informatics faculty of St. Mary's University, for the success of the research work in one way or the other.

List of Acronyms

ATM:	Automatic Teller Machine
BS:	British Standard
CBS:	Core Banking Solution
CCTV:	Closed Security Television
CIS:	Center for Internet Security
COBIT:	Control Objectives for Information and related Technology
CS:	Cyber Security
CSA:	Cyber Security Auditing
CSAF:	Cyber Security Auditing Framework
CSAS:	Cyber Security Auditing Standard
CSF:	Cyber security Framework
GASSP:	Generally Accepted System Security Principles
ICT:	Information Communication Technology
IEC:	International Electro technical Commission
INSA:	Information Network Security Agency
IT:	Information Technology
ITGI:	Information Technology Governance Institute
ISACA:	Information Systems Audit and Control Association
ISO:	International Standardization of Organization
MCIT:	Ministry of Communication and Information Technology
NBE:	National Bank of Ethiopia
NIST:	National Institute of Standards and Technology
PCI-DSS:	Payment Card Industry Digital Security Standards
SCSAP:	Simple Cyber Security Audit Process
SPSS:	Statistical Product and Service Solutions

LIST OF FIGURES

LIST OF TABLES

Abstract

The advancement of cyber security and technology offers a vital benefit for business. Modern Banking increasingly relies on the Internet and computer technologies to operate their businesses and market interactions. Banks are on the way of using up-to-date 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 cyber systems. The threats and security breaches are highly increasing in recent years globally. Ethiopian case is not an exception.

The main objective of this study is to propose and develop a workable Cyber Security Auditing Framework (CSAF) in banking sector. In this work, attempts were made to examine and compare the available cyber security frameworks and best practices. This research combines ISO audit checklists and expert experiences to assess the cyber security system practices in the banking industry.

By applying a mixed research method approach the study assesses the existing practices, process and challenges of the selected banks cyber security issues and proposed cyber security audit framework which is workable for the Ethiopian banking industry. The framework is constructed from two basic pillars. The first is the requirement identification mechanism which is further broken into ERM (Entity Relation Model) and organizational & process models. The second one is the counter measure which focuses on the organizational policy, procedure, guideline, and controls. Finally, the researchers proposed a workable framework that can assist the industry from cyber-attacks.

The framework has both practical and theoretical contributions to the industry at large and for researchers for further similar efforts.

Keywords: *Cyber Security, Cyber Security Auditing, Cyber Security Auditing Framework, Security Threats, and Security controls.*

Contents Page

CHAPTER ONE - INTRODUCTION

1.1 Background of the Study

Cyber security (CS) is, basically, the process of ensuring the safety of cyberspace from known and unknown threats. The International Telecommunication Union states that cyber security is the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, and assurance and expertise that can be used to guard the cyber system, organization and related assets [18]. Cyber security (CS) is important because government, military, corporate, financial, and health organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that is intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences [25].
For an effective cyber security, an organization needs to coordinate its efforts throughout its entire cyber system .Security counter measures help ensure the confidentiality, availability, and integrity of cyber systems by preventing asset losses from cyber security attacks [8]. Effects of cyber security failure leads to the loss of intellectual property, direct financial loss from cybercrime, loss of sensitive business information, sabotage of operations, extra costs for systems' recovery, stakeholders loss of on system confidence.

Cyber Security Auditing (CSA) is an independent review and examination of system records, activities and related documents. These auditing are intended to improve the level of cyber security, avoid improper cyber security designs, and optimize the efficiency of the security safeguards and security processes. It is a systematic, measurable technical assessment of how security policies are built into the cyber systems and it is part of every successful cyber security management [26].

The major challenge in cyber Security in banking industry is the knowledge gap about the holistic approach of cyber security management, 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 in most of the bank industry [22].

Some of the 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 cyber security [4].

Literature in the area of cyber security shows that security culture is still in its early stages of development especially in developing countries. Thus, the establishment of an organizational cyber security culture is necessary for effective cyber security [22].

Ethiopian IT capacities are still at a developmental phase and are immature in relation to leading western technologically developed countries. In addition, the business environment of Ethiopian is different from the business environment in the USA and other Western countries [22]

Cyber Security Framework (CSF) is a set of industry standards and best practices to help organizations manage cyber security risks. It is basically, a blueprint for building a cyber-security program to manage risk and reduce vulnerabilities. The Framework enables organizations – regardless of size, degree of cyber security risk, or cyber security sophistication – to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. [25].

Cyber-attack involves the malicious application of information and communication technology either as a target or as a device by several malicious actors. Cyber security could also refer to the security of internet, computer networks, electronic systems and other devices from the cyber-attacks.

Research in Ethiopia indicates that, there is lack of cyber security auditing framework and practice. For instance the research done in the investigation of the state of cybercrime in Ethiopia by taking 40 institutions from Financial Organization of Ethiopia found that all respondents experienced a number of cybercrime incidents, Computer viruses, worms, malware, or other malicious attacks (57.1 %), website defacement (40%), illegal access (17.1%), and spam (14.7%) were the most frequently penetrated cybercrimes against the organizations. The respondents also indicated a range of infrequently occurring cybercrimes such as causing damage to computer data (62.9%), denial of service (DOS) (45.7%), and system interference (45.7%). Overall, the survey results demonstrate that cybercrime is a legitimate problem in Ethiopia. When one takes into account institutions' lack of capability regarding cybercrime detection, it is valid to presume that cybercrime in Ethiopia is more prevalent than what is revealed in this survey. A majority of the respondents (77.1%) also said that they do not have any organizational

structure specifically dedicated to dealing with cybercrime threats. Only 8.6% of the institutions (four banks) have specialized teams responsible for cyber security incidents. These results demonstrate that cyber security governance is neglected by the majority of the institutions involved in the survey. The results may indicate that institutions as a whole are ill-prepared to deal with cybercrime [12].

This research work propose a workable cyber security audit framework that can be used to guide the banking industry by , assessing the current practice, and challenges, which at the end helps the banking industry as guideline for cyber security auditing process of the industry.

1.2 Statement of the Problem

IT plays a vital role in modern banking industry across the world. The banking industry in Ethiopia is one of the rapidly growing sectors of the country's economy. In addition, the banking service has also dramatically changed from manual operation to the technology supported system which then brought the industry and customers to national and global presence anywhere-anytime banking. The banking business competition has motivated the advancement of services enabled by IT which in turn increased the cyber security risk. These threats to data's and information can include purposeful attacks, environmental disruptions, and human or machine errors and result in great harm to the national and economic security interests of the country [29].

Most of the Ethiopian bank industries face challenges with regard to the governance of cyber security resources mobilization process across all. Most researchers also indicate that there need rigorous research for the proper security enhancement mechanism through designing a guide line that can support the task of security protection.

According to [42], most of the Ethiopian Bank industries are also challenged in managing their ICT resource .This industries in Ethiopia lacks security policy document, security protection manual documents. The researcher also identified that most of the banks don't conduct any cyber security awareness and training for their staff. He concluded that the capability and readiness of Ethiopian government organizations to perform cyber security audits is extremely low.

Ethiopian banking system is still underdeveloped compared to the rest of the world regarding electronic payment, internet banking, telephone banking, online shopping etc. Such systems are at an embryonic or infant stage. The reason for this weak or evolutionary development is being numerous, the main one that is cited by different scholar is security threats or poor implementation of cyber

security in the country [18] [37] Currently, for banking industry there is no cyber security standards provided and there is no clear guidance regarding what would constitute an acceptable minimum baseline body of cyber security knowledge for end users in the country [18].

The preliminary literature survey shows organizations in Ethiopia are at different level of understanding and acting with regard to security auditing and various threat mitigation. There is no standard format to conduct a cyber-security audit framework by the regulatory body and to follow up the work done by other external parties in case of outsourcing cyber security audit framework task to the third parties[18].

In addition, from my preliminary investigation it was revealed that 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 cyber security framework which serve as a guide to develop and implement their own cyber security auditing based on their own requirement in line with the valid national cyber security policy, besides lack of skilled manpower, security management resources and finance [15].

1.3 Research Questions

The study intended to address the following research questions:

- What are the existing practices and processes of cyber security auditing and the methods, techniques, standards and tools used in Ethiopian banking sector
- What are the major challenges that the Ethiopian banking sector are facing on cyber security management.
- What framework can support Ethiopian banking industries to perform effective cyber security auditing and ensure that cyber resources are well protected?

1.4 Objective of the Study

1.4.1 General Objective

The general objective of this study is proposing a cyber-security auditing framework that enables bank industries to perform effective and efficient cyber security auditing.

1.4.2. Specific Objectives

The specific objective of the research included:

- assess the existing practices and process of cyber security auditing systems and the methods and techniques used in selected Ethiopian banks
- identify variations in cyber security systems and process and major causes of their variations.
- identify the predominant problems that impedes the cyber security auditing process in the banking sector in Ethiopia.
- assess different cyber security frameworks which are done by different scholars across the world.
- propose a cyber-security auditing framework that can address the current challenges and, standardize the process of cyber security management, this can be applied in Ethiopian bank sector.
- validate the framework based on the actual environment

1.5 Research Methodology

1.5.1 Research Approach

In order to attain the general and specific objective, the research applies a mixed method research approach combining both qualitative and quantitative methods. In the qualitative aspect the general knowledge of the experts in managing cyber security issues are investigated and in the quantitative aspect the existing practices, resource requirement, the kind of training, the experts have and research methods will be assessed [40]. The combination of different research approaches and datasets is a form of methodological pluralism [37], which itself is a way to increase the validity of the study results. Methodological pluralism allows the researcher to observe the phenomenon from different viewpoints and also to combine the advantages of two different approaches.

1.5.2 Study Population

The overall population of the study concentrates on the head quarter of selected banks of Ethiopia located in Addis Ababa. The researchers assumed that there is difference in the characteristics of the overall selected companies profile in terms of technology usage, staff composition, resource, service coverage and service year. The selection of the company is based on purposive sampling, due to the interest of individual companies in terms of willingness in conducting research in their company.

1.5.3 Data Collection

The data is collected from both primary and secondary sources specifically; questionnaire and interview as primary data source and observation of the existing infrastructure, documentation, policy manual are also seen as secondary data sources

1.5.4 Data Analysis

The collected data from the questionnaire are summarized using SPSS version 20 and later on represented by different statistical methods such as percentage, using tabulation, charts and frequency distribution. The findings from qualitative data gathered through interview will be coded and summarized and triangulated for the findings of the survey data.

1.5.5 Designing a cyber-security auditing framework

Designing the cyber security auditing framework includes all the relevant aspects of cyber security auditing process that enable to solve the existing cyber security problems and challenges. The framework mainly focuses on addressing the existing challenges that the bank industries are facing and possible remedial solutions derived from the empirical research and literature will be seen critically. The evaluation for the designed framework will be done by selecting relevant organization senior experts to check for the validity of the framework relating with their best experience, challenges and the international standards through designing survey questions.

1.5.6 Validation

Validation on the final output of the research is made through distributing a questionnaire at some selected banks that have better experience and experts to provide valuable comments.

1.6. Scope of the Study

The scope of this research mainly focuses on proposing a workable cyber security auditing framework that can serve as guideline for banking sector in Ethiopian to overcome cyber security risks by focusing on the existing practices, challenges, methods, techniques currently applied in Ethiopian banking sectors.

1.7. Significance of the Study

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

- The study shall serve as a guideline for developing and implementing cyber security auditing framework in banking industry in Ethiopia.
- It enables all banks to have a common cyber security framework in Ethiopia.
- It adds a new way of thinking in the existing body of knowledge.
- It also serves for practitioners and researchers to conduct more comprehensive research in cyber security management.

1.8. Limitation of the Study

The result of the research would be more comprehensive if it covers the entire Banks and their branches in Ethiopia. However, due to time constraints the researcher only focused on headquarters of selected banks.

1.9. Organization of the Thesis

This study is organized in six chapters. These are:

Chapter One: focuses on the background of the study, statement of problem, objectives and significant of the study.

Chapter Two: is the literature on cyber security, Auditing activities and implication process, Cyber security auditing standards (CSAS), and Tools, Cyber security Audit Frameworks, Basic criteria to assess cyber security audit readiness, and presented for further description of the research area. Related works are presented.

Chapter Three: this chapter presented research design and methodology which includes general insight on the existing research methods, 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 focuses on a new proposed Cyber Security Auditing Framework (CSAF) clearly presented.

Chapter six: focus on conclusions, recommendations and future works of the study.

CHAPTER TWO - REVIEW OF LITERATURE AND RELATED WORKS

2.1. Introduction

In this chapter, the researcher has tried to review the Overview of Cyber Security Auditing Framework (CSAF) and its theoretical and empirical framework in a bank sector. The reviewed points are: Overview of Cyber Security, Auditing Activities and implication process, Cyber security Auditing (CSA), Steps and procedures for security Audit, Cyber security Auditing Standards and regulations, Cyber security Audit Frameworks (CSAF), Cyber Security Auditing Tool.

2.2. Overview of Cyber Security (CS)

Cyber security 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. [23] .The application of information technology has brought about significant changes in the way the institutions in the banking sector process and store data. This sector is now composed to face various developments such as internet banking, mobile banking, e-money, e-cheque, e-commerce etc., as the most modern methods of delivery of services to the customers. However, Customers are very concerned about privacy and identity of theft. [32]. Business partners, suppliers, and vendors are seeing security as the top requirement, particularly when providing mutual network and data access. Banks' ability to take advantage of new opportunities often depends on their ability to provide open, accessible, available, and secure network services.

Having a good reputation for safeguarding data's and information's will increase market share and profit [23].Banks are clearly responsible for compromised data in their possession that results in fraud. Therefore, banks have to be responsible for fraudulent activity perpetrated via the internet channel [23].

Telecommunication networks have played a catalytic role in the expansion and integration of the Cyber Security (CS), within and between the institutions, facilitating data accessibility to different users. In view of the critical importance of Cyber Security (CS), there is a need to exercise constant vigilance for the safety of the financial systems. Structured, well defined and documented security polices, standards and guide lines lay the foundation for good cyber security.

2.3. Cyber Security Management

Cyber Security management is the process of protecting electronic and non-electronic information assets against the risks of loss, misuse, damage, and disclosure or corruption [17].

ISO/IEC 27002:2005 is an international standard, refers to a code of practice for cyber security management, and is intended as a common basis and practical guideline for developing organizational security standards and effective management practices [17]. According to [9] this standard contains guidelines and best practices recommendations for these 10 security domains. Implementing a Cyber Security Management System involves with 3 key aspects of an organization; physical and environmental aspect, Management aspect and Operational aspect. Hence, the concept denotes those 3key aspects in the bank related to the direction and control of the cyber security over information assets.

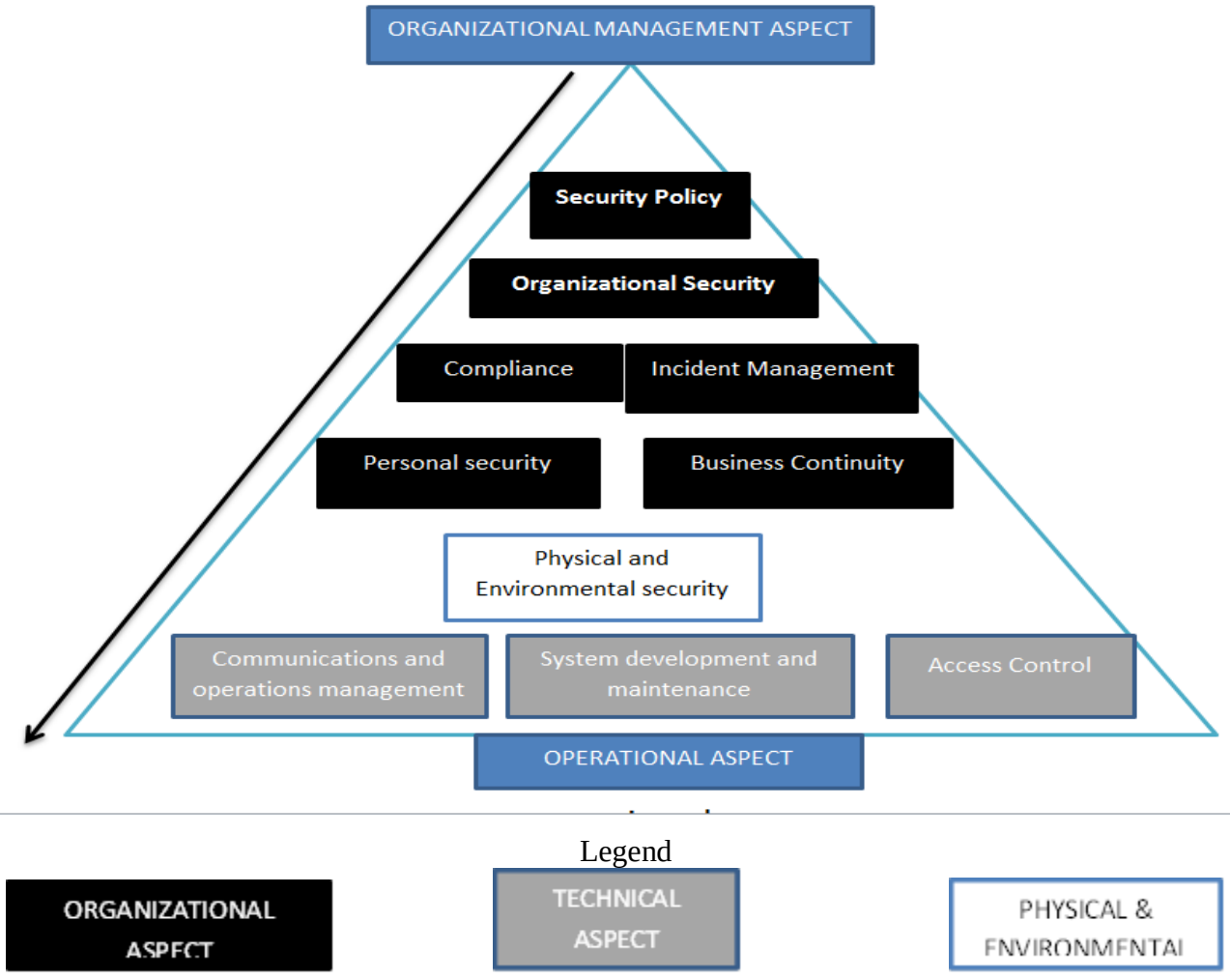

Figure 2.1 Fredrik, 2005

2.4. Auditing activities and implication process

Auditing is a systematic independent examination of the data and the environment to ascertain whether the objectives, set out to be met, have been achieved. Auditing is also described as a continuous search for compliance [41]. The auditors may not necessarily examine the entire system; they may examine a part or parts of only. Auditing covers primarily three broad major areas of activity. Gathering of information, comparison of information and asking why [39]. But a basic purpose of any audit is to identify control objectives and the related preventive, detective and corrective controls that address the objective [20]. As Cyber Security (CS), auditor should understand the various types of auditors and the associated audit procedures for each. Three types of audit are [33].

Financial Audits: The purpose of financial audit is to assess the correctness of financial statement of records. The Cyber Security (CS) auditor will often use computer assisted procedures to support financial auditors in these types of audit.

Operational Audits: An operational Audit is designed to evaluate the internal control structure in a given area. Internal Auditors are associated most often with operational audits. Many Cyber Security (CS) audits, including reviews of application controls or of logical security systems, are operational in nature.

Comprehensive Audits- it combines both Financial and Operational Audit steps. The planning phase should be a joint venture involving Cyber Security (CS), Financial and Operational Audits. A comprehensive would include both compliance and substantive audit steps.

2.4.1. Cyber Security Auditing (CSA)

Cyber Security Auditing(CSA) is an independent review and examination of system records, activities and related documents to determine the adequacy of system controls, ensure compliance with established security policy and approved operational procedures, detect breaches in security so as to verify whether data integrity is maintained, assets are safeguarded, organizational goals are achieved effectively and resources are used efficiently. CSA is a systematic, measurable technical assessment of how security policies are built into the data systems. [26] CSA is part of every successful cyber security management [35].

The CSA is therefore a tool for determining, achieving, and maintaining a proper level of security in an organization. The audits are intended to improve the level of cyber security, avoid improper cyber security designs, and optimize the efficiency of the security safeguards and security process [35]. The

CSA differs from the traditional audit in the sense that it requires adequate knowledge of computer systems in addition to the basic concepts of normal auditing.

In general, the CSA, as anew auditing discipline, places emphasis on a holistic examination of cyber security. This means that all levels, from the establishment of cyber security organization through personnel issues to system configurations, are checked [31].

2.4.2. Steps and procedures for cyber security Audit

According to different scholar's perspective, there are different approaches of audit process and procedures to achieve cyber security audit needs, but almost all have its own commonality. For the sake of clarity, we can see the following different approaches which are proposed by different researchers and organizations.

According to [42] [5] the Simplest Cyber Security Audit Process (SCSAP) is a dynamic security audit approach based on both BS 7799.2 and ISO 17799. A security standard is regarded as a control system where on iterative control mechanism simulates standard compliance inputs to produce a CSA design that translates the initial security audit objectives. SCSAP consists of the following phases:

1) Security Audit; 2) planning; 3) Review of policy; 4) Normal Audit; 5) Technical Audit; 6) Data Analysis; 7) Risk Analysis; 8) Report; and 9)Post-Audit. These are the same steps found in any other security audit methodology reported in the literature [30]. In addition[36] proposed an audit process in seven steps at figure 2.1[36] , the input data are log file, Intrusion detection systems report and data from the system, and deliverables from those steps of audit are vulnerability report, threat/risk assessment report and audit report. This deliverables are ultimately meant to address the security holes by addressing weakness in different aspects of systems which could be technical, human resources issue or policy cases, etc., [42]. But the audit process is limited by the following seven steps:

(1) vulnerability scanning - scanning the infrastructure,
(2) report audit - auditing reports like logs, intrusion detection systems reports, etc.,
(3) security architecture audit - auditing the existing security architecture,
(4) baseline auditing - auditing the security setup to verify that it is in accordance with the security baseline of the organization,
(5) internal control and workflow audit - auditing the existing work-flow,

(6) policy audit - auditing the security pol-icy to ensure that it is in line with the business objective and

(7) Threat/risk assessment – assessment of the various risks and threats facing the company's information systems [2].

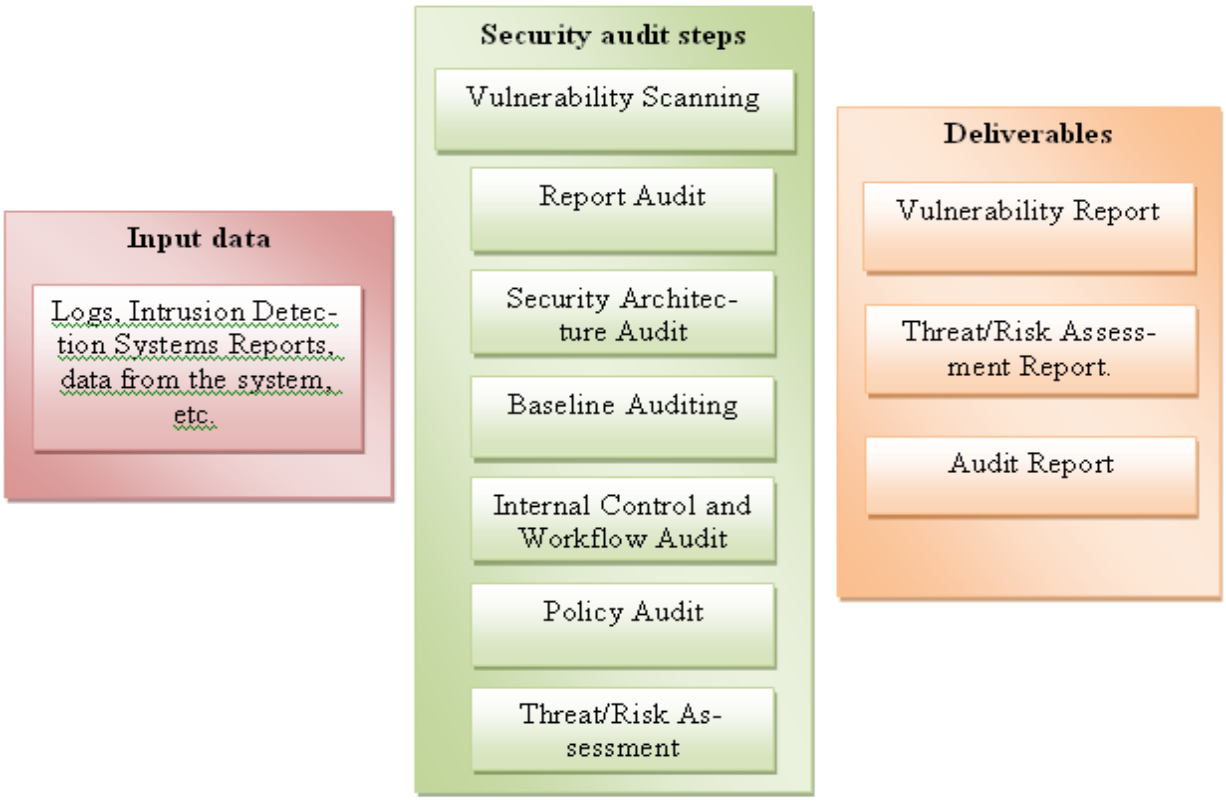

Figure 2.2 Security audit steps

During and at the end of the auditing process a series of reports may be elaborated: a report with the vulnerabilities identified in the organization cyber system, a report with the threats and risks the organization faces as a result of the existing vulnerabilities including faulty policy, architecture, etc., and an audit report which gives the security overview and the results of all the audits [2].

Another perspective on the security audit process is provided by [28] which divide the audit in six steps:

(1) Planning - to determine and select effective and efficient methods for performing the audit and obtaining all necessary information;

(2) collecting audit data - to determine how much and what type of information to be captured, and how to filter, store, access and review the audit data and logs;

(3) performing audit tests - general review on the existing security policies or standards(security configurations)Technical investigation;
(4) reporting for audit results – present the current security environment;
(5) protecting audit data & tools - safeguard the audit data and tools for the next audit or future use;
(6) Making enhancements and follow-up - make corrective actions if required.
(7) The security audit process is becoming more difficult to undertake with the growing complexity of information systems.

2.5. Cyber Security Auditing Standards (CSAS)

Institutions and professional bodies all over the world have issued various standards, guidelines and best practices regarding cyber security from time to time. Those standards and guidelines prepared based on problems that rose around security, from professional bodies; British standards (BS 7799), International Organization for Standardization ISO/IEC, Center for Internet Security (CIS), Generally Accepted System Security Principles (GASSP), National Institute of Standards and Technology (NIST) and Information System Audit Control Association (ISACA) are some of known organizations in the world on cyber security auditing standardizations. The Standards that are proposed by the above organizations are many in number but due to the scope of this thesis I focus on those standards which are used to implement cyber security audit framework for banking sector.

2.5.1International Organization for Standardization (ISO)

ISO/IEC; 27002:2005: Which is previously named ISO17799 standard, developed by the ISO in collaboration with IEC. It is considered as code of practice for cyber security management [17] and is intended as a common basis and practical guideline to develop a common organizational standard and effective management practices used to ensure organizational objectives. ISO/IEC 27002:2005 provides best practices recommendations for those in charge of initiating, implementing and managing cyber security [17]. This standard has originated from BS 7799; 1, which was developed by the British Standard Institute BSO. According to[31] ,ISO/IEC 27002 contains security recommendations for 12 security domains among these , a total of 39 control objectives and hundreds of best- practice cyber security control measures are recommended for organizations to satisfy the control objectives and protect information assets against threats to CIA, see figure 2.2[2] which includes:

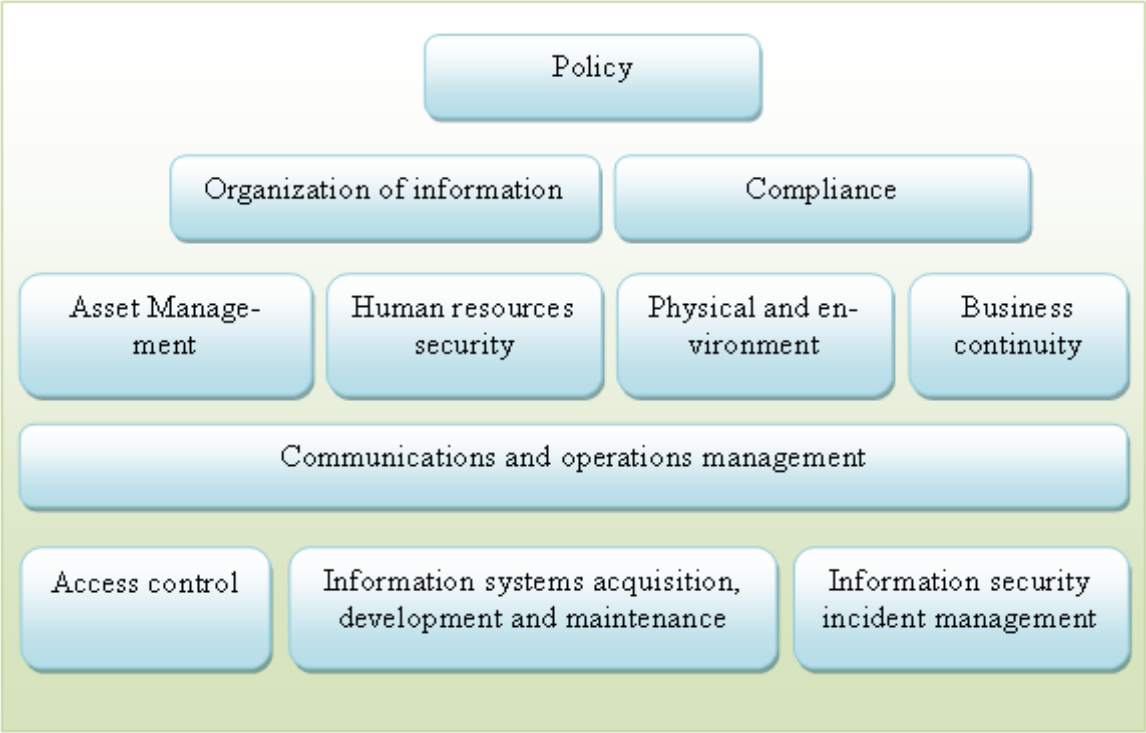

Figure 2. 3. *Relationship between the control clauses*

1. Security policy and standard - management direction;
2. Organization of cyber security - governance of cyber 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. Cyber 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.

This standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's Cyber Security Management System (CSMS).

Cyber security auditing in a given organization needs to consider the status of the domains numbered from 4-15 and their sub-domains depicted in figure 2.4[17] with respect to the objectives, resource availability, and other issues relevant for a particular organization[42][17].

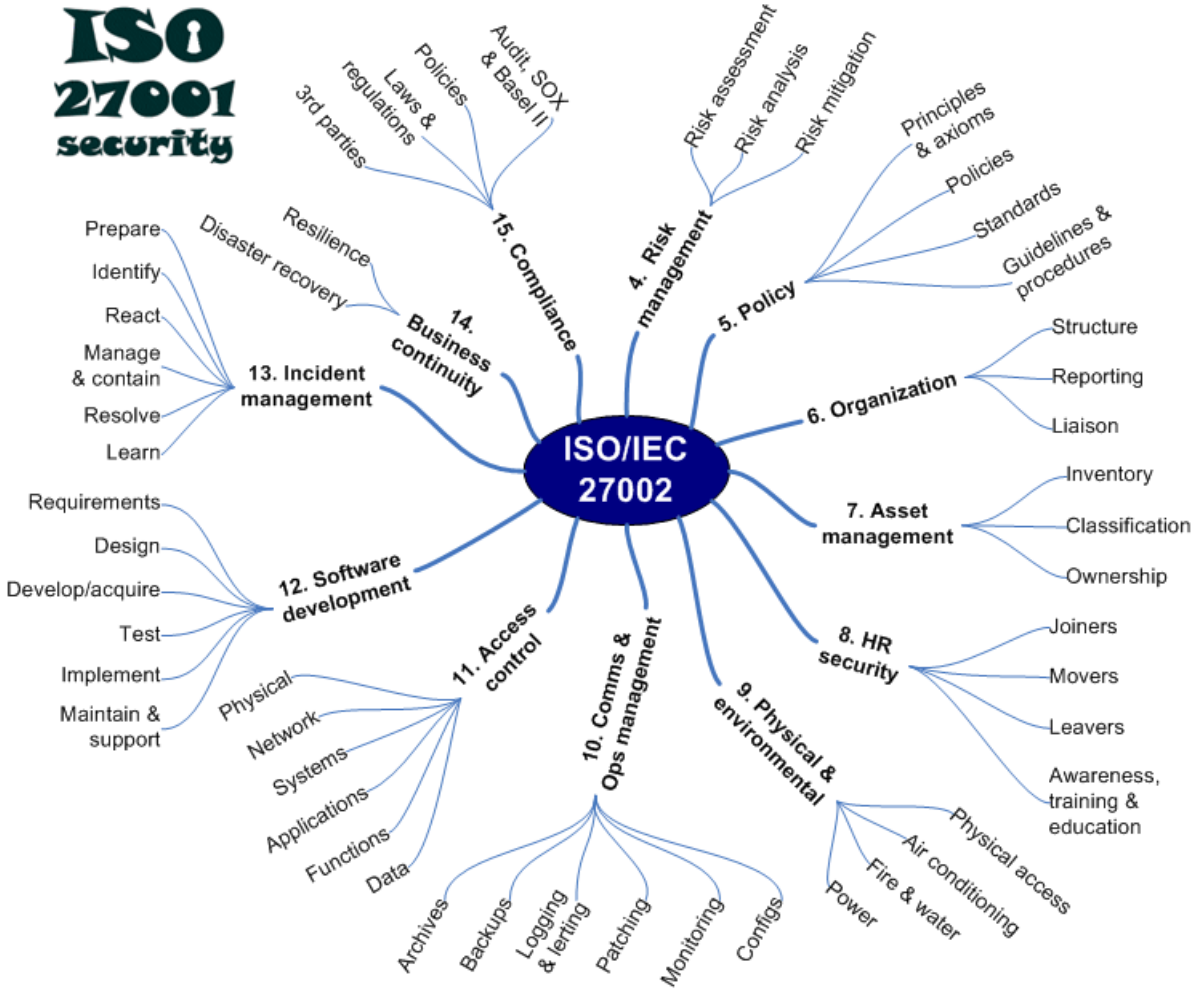

Figure 2.4.: Main domain of ISO/IEC 27002 security standard

ISO/IEC 27001:2005 is its use in the internal and external auditor of organizations to determine the degree of compliance with the policies, directions and standards adopted by an organization [17], it specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintain and improving a documented cyber security management system within an organization.

This standard is usually applicable to all types of organizations, including business enterprises, government agencies, and so on.

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

PCI-DSS is a worldwide cyber security standard defined by the Payment Card Industry Security Standards Council [13]. 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 [13]. This standard encompasses a group of principles for security management, policies, procedures, network architecture, software design and other critical protective measures [16].Generally; it is security controls for credit card transactions.

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

COBIT is a set of practices(framework) for IT management, created by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996 [13] 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 [13]. It presents an international and generally accepted IT control framework enabling organizations to implement an IT governance structure throughout the enterprise [42]. 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 [19]. The COBIT 4.1 framework explains how IT processes deliver the information that the business needs to achieve its objective. This delivery is controlled through 34 high-level control objectives, one for each IT process, 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 [16].

2.6. Cyber Security Auditing Tool

The cyber security audit tool identifies the four essential process of our developed tool for cyber security audit service. For instance functions are: identifying, protecting, detecting, responding and recovering any event of cyber attacks into organizations. Such methodological approach was seized from NIST Framework [24]. Among the functions we additionally added several other categories, which in our opinion were missing from the framework and will lead to customer's needs. And at the same time to bring more value and to be in fact beneficial and efficient by covering the latest technologies and threats, such as, bring your own device (BYOD), human factor, etc.

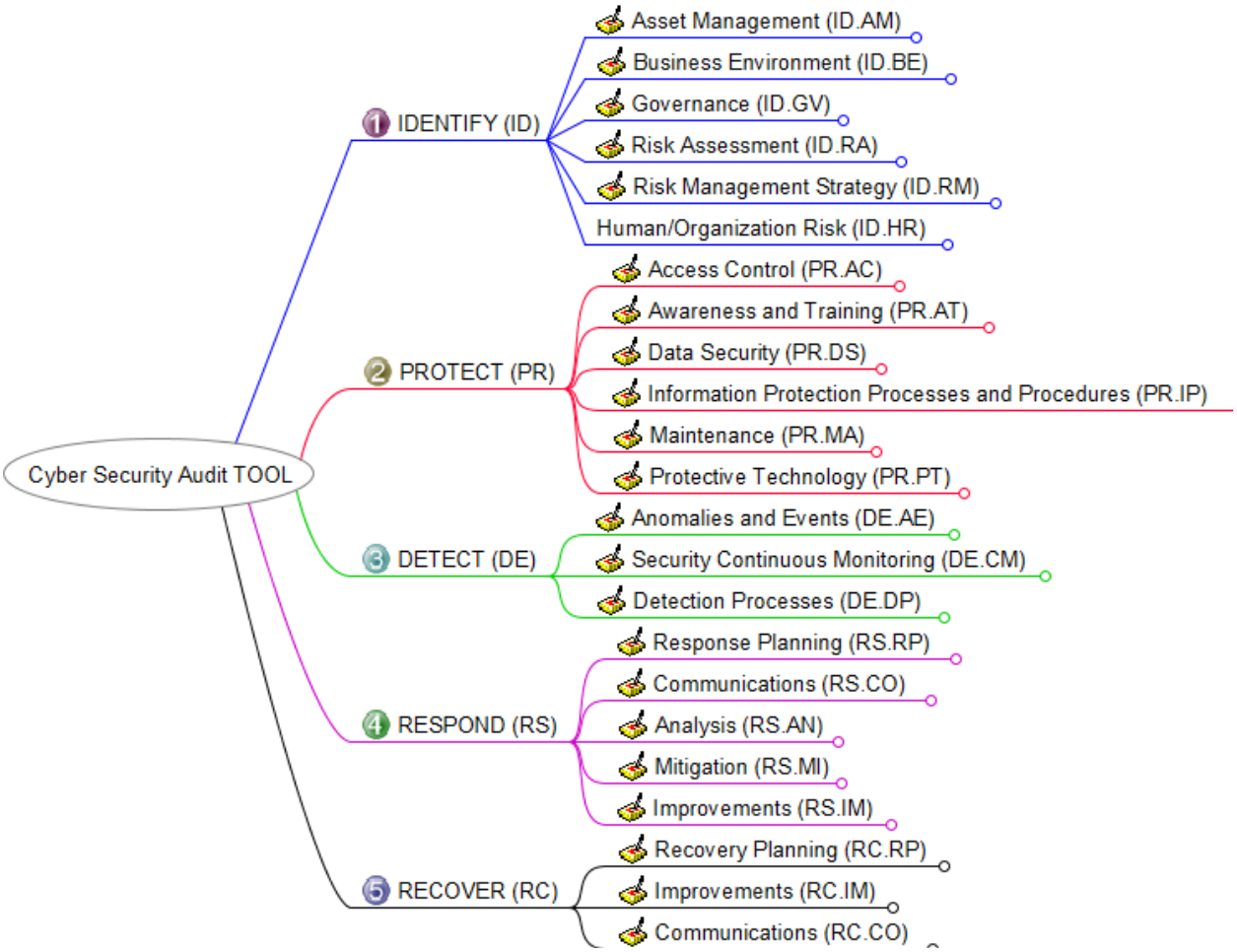

Figure 2.5 Cyber Security Audit TOOL map

2.7. Cyber Security Audit Frameworks (CSAF)

The phrase "Security framework" has been used in a variety of ways in the security literature over the years, but in 2006 it come to be used as an aggregate term for the various documents (and some pieces

of software), from a variety of sources, that give advice on topics related to cyber security, in particular regard to the planning, managing, or auditing of overall cyber security practices for a given institution [34]

Framework for CSA consists of multiple level of guidance, which consists of polices, standards, procedures, principles, breakdown structures, audit guidelines/outlines, Legislations. Reporting standard and product evaluation [34] they are components that are always assessed while conducting security audit in a certain setting.

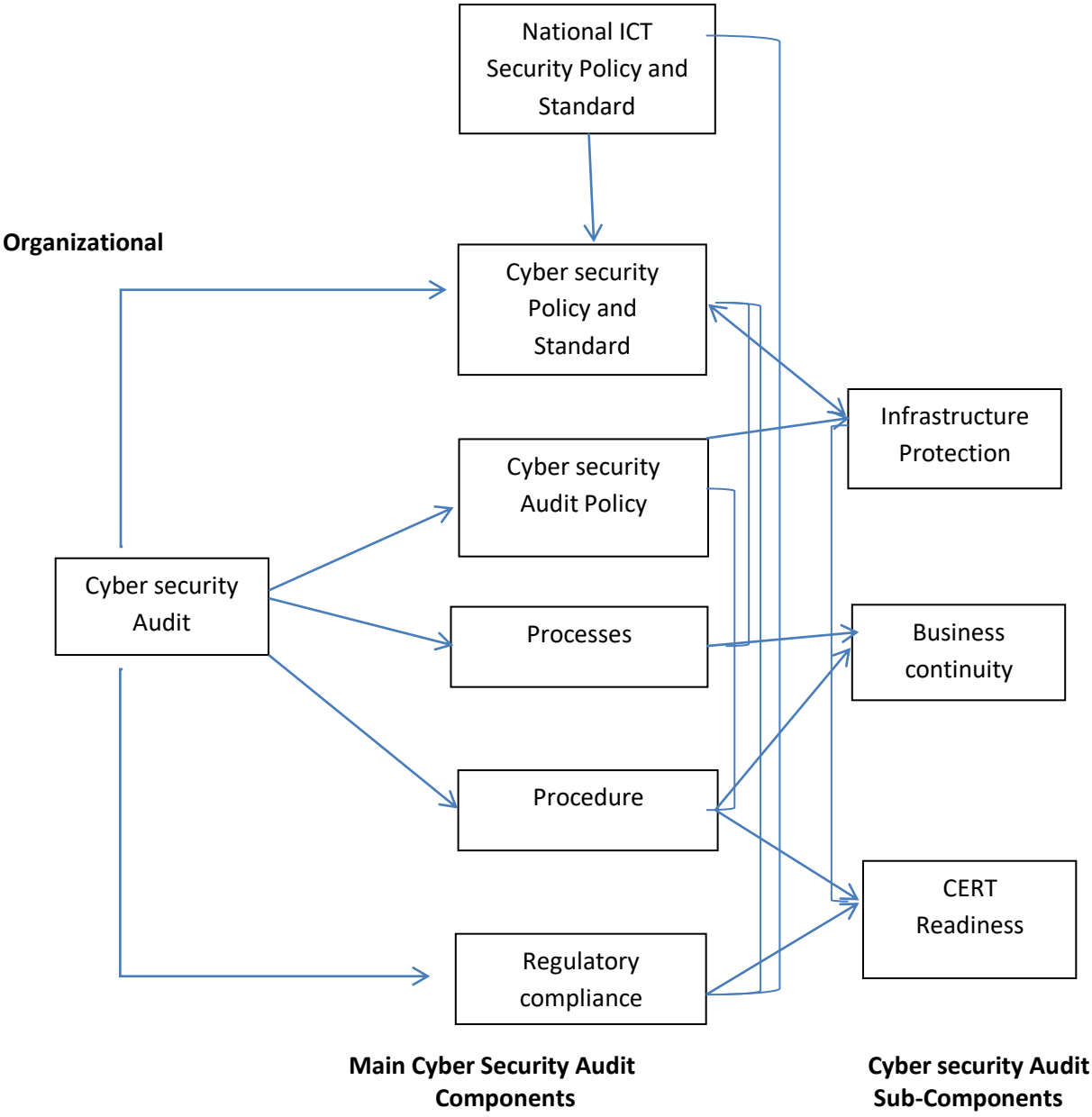

Figure 2.6: Onwubiko cyber security audit framework

The standard in the framework refer to mandatory requirements that security systems at organization or national level need to meet. For example, Cyril Onwubiko has developed a full- fledge cyber security audit framework, which addresses five main components and three sub-component of security, refer figure 2.5[26]

The components comprises: security policy that defines acceptable use, technical controls, management standards and practices. Audit policy that specifies what needs to be audited processes which are organization process around security; procedures that organization engages in order to protect its valued asset; Regulatory compliance that stipulates acceptable regulatory and security compliance for the organization in its given environment. Sub-components included infrastructure protection plan, business continuity plan and computer emergency response team readiness plans and practices for incident response [26].The components each has direct relations to the three sub components as shown in figure 2.5 above.

There is also plenty of management and enterprise architectural security frameworks are available in the world, those give a better direction to create or model new frameworks for any kinds of problems. The architecture framework should be able to be modified and add value in future applications based on organizational growth and needs [11].Many sustainability standards have been developed and will be developed in the future, However, information model in the standards and relationships among standards are hard to describe and understand because of their complexity. After a thorough review of management and enterprise architectural frameworks it is shown that ZACHMAN framework is a best fits to plan security architecture for an enterprise as any evolving changes in technology can be implemented onto the ZACHMAN framework without affecting the direction of the enterprise. The ZACHMAN framework can contribute to understanding and describing complex relationships and information models in sustainability standards [14]. Therefore, the security planning using the ZACHMAN framework applied to enterprises is helpful for sorting out complex technology and methodology issues that are significant both to general and technology management[7].A framework was developed by John ZACHMAN, in 1980, which is a two- dimensional classification schema diagramed in a six-by-six matrix format as shown in figure 2.13[41].The rows represent the perspective of different players in the process (Planner, Owner ,Designer, Builder , Sub-contractor, the system) while the columns represent aspects of the process (Data, Function, Network, People, Time, Motivation).The thirty-six frames at the core of the integrated framework are referred to as cells. In this model, each cell is unique. The columns manage the complexity while the rows manage

the changes [41]. The framework is comprehensive, primitive, and generic and distinguishes an issue by answering all the six primitive linguistic interrogative questions who, what, where, when, why, and how, hence they cannot be fragmented further after analyzing. In addition to this, it is a logical structure for descriptive representations (i.e. models, or design artifacts) of any complex object and it is neutral with regard to the processes or tools used for producing the descriptions. Therefore, the framework as applied to enterprises is helpful for sorting out very complex technology and methodology choices and issues that are significant both to general management and to technology management. This makes the framework generic [41] [11].

Figure 2.7 ZACHMAN Enterprise Architectural Framework

The framework come up with a set of seven rules: These are, Rule 1. The columns have no order, Rule 2. Each column has a single generic model (Every column can have its own meta model) Rule 3. The

basic model of each column must be unique, Rule 4. Each row describes a distinct, unique perspective, Rule 5. Each cell unique, Rule 6. The composite or integration of all cell models in one row constitutes a complete model from the perspective of that row and Rule 7. The logic is recursive [41].

The basic idea behind the ZACHMAN framework is that the same complex thing or item can be described for different purposes in different ways using different types of descriptions(e.g. textual, graphical)[27]. Security is a never- ending process that requires constant monitoring, updates, investment, research and implementation of new technologies. The ZACHMAN framework is based on an open architecture, which ensures solutions that can be easily extended to an enterprise's security policy of today and that of the future [7].

2.8. Basic Criteria to assess Cyber Security Audit readiness

This research began with assessing the basic issues that needs to be addressed during survey, in order to identify the readiness of banking sector. Based on this research question, twelve minimum security requirements stated commonly by scholars have been identified. In building cyber security audit capability, management should assess the organization's cyber security audit readiness by taking into account the relevant factors discussed below. In many instances, this process will determine what is practical to implement within a given time and budget constraints [14]. Based on NIST[32], ISO 27002 [17], ICT readiness check list for developing countries[32] and formulation of IT Auditing Standards by [14], the minimum security requirements cover 6 generally accepted security- related areas in order to check the confidentiality, Integrity and Availability of cyber systems on three state: information in processes, at rest and on transmittal. These minimum security requirements and interview results from IT and security auditors are presented as follows.

1. Security Policy and Standards

   The organization's security policy is the set of laws, rules, and practices that regulates how an organization managers, protects, and distributes resources to achieve specified security objectives [23]. These laws, rules and practices must identify criteria for individual's authority, and many specify conditions under which individuals are permitted to exercise their authority to be meaningful, these lows, rules , and practices must provide individuals measurable ability to determine whether their actions violate or comply with the policy[14].

2. Organizational security

Organizational security has been seen from the perspective of existence of management forum that ensures the management support to cyber security. This could be the work given to a unit or on individual, who work with the IT organization to acquire appropriates tools and implement the right processes which implements the security policy. They are additionally responsible for providing the initial and refreshes training to the staff and address security incidents. There is also a need to ensure that the date of the organization that is accessed by or transferred to external organizations is suitably protected [14].

3. Human resources (personnel) security

Employees handling, personnel data in an organization need to receive appropriate awareness training and regular updates in on effort to safeguard the data entrusted on them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organization's security policy [14]. The management of human resources security and privacy risks is necessary during all phases of employment association with the organization. The three areas human resources securities are: pre-employment, during employment and termination on change of employment.

4. Communications and operations Management

An organization needs to keep track of the process and procedures they use for their business operations. This includes the set of organizational procedures and process that insures the correct processing of data in the organization, and the documenting procedures for media and data handling, emergency procedures, network security logging and backup procedures. The objective of this category is to insure the correct and secure operation of IT processing facilities. Controls should be in place to secure all the three stages of data communication .i.e. assembly, dispatch and retrieval of the data in a network.

5. Physical and environmental security

Physical security describes measures that are designed to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource or stored information; and guidance on how to design structures to resist potentially hostile acts. Physical security can be as simple as a locked door or as elaborate as multiple layers of barriers, armed security guards and guardhouse placement [14].Physical security is primarily

concerned with restricting physical access by unauthorized people(commonly interpreted as intruders) to controlled facilities.

6. Access control

Access control refers to exerting control over who can interact with a resource. Often, this involves an authority, who does the controlling [42]. The resource can be a given building, group of buildings, or computer based IT system. Access control is in reality an everyday phenomenon. A lock on a car door is essentially a form of access control. The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment. Access security encompasses control on access to information, prevention of unauthorized access to information systems, authorized user and computer access, protection of network services,, detection of unauthorized activities and providing security during computing and tele-working processes [14]

2.9. Related Works

One of the related works done on "Cyber security culture in the banking sector in Ethiopia" by [1] The purpose of this study was to investigate the extent of the cyber security culture of Ethiopia and indicated that, ever big banks in the world that generally do better job of security are found to be victims of security breaches. This research conducted on Ethiopian banking industry on case of 4 banks head office. The methodology they have used to conduct the research was a mixed method research approach in which both qualitative and quantitative method is applied; the survey result indicates that, only 32% of the industries have proper information security governance is implemented. The level of readiness among employees to embrace cyber security changes shows a slightly promising (38%). As per the researchers' conclusion, the dimensional frequency analysis shows holistic and strategic work is needed to promote cyber security culture in the banking sector in Ethiopia, and cyber security culture is unsatisfactory. Consequently the level of proper information security governance in the banking sector in Ethiopia is a critical area of improvement. Finally, they recommended that there is also a significant space to enhance the trust environment between managers and employees that can promote change in cyber security culture and more rigorous researches are needed to frame practical strategies for the mitigation the possible cyber security breaches so as to enhance the cyber security culture of the banking and other industries in Ethiopia [1].

According to [42], "Cyber security audit readiness in case of Ethiopian government organization. The study aimed at identifying the cyber security audit readiness of Ethiopia governmental offices The researchers' used a mixed research method approach. The result of his analysis was based on the responses obtained from 8 Ethiopian government organizations; those are the main organization selected by the government through the MCIT for the first phase implementation of e-government service delivery. The findings from the research shows that 56.25% of the organizations surveyed have no security policy document while the rest of them do have some level of security protection manual documents, which they cascaded and adopted from the national ICT security policies and standards. But when it comes to implementation, none of the organizations have implemented the policy.68.75% of the respondent organizations never conduct any cyber security awareness and training , security roles and responsibilities are not defined and documented in 62.5% of the organization. In general, he concluded that the capability and readiness of Ethiopian government organizations to perform cyber security audits is extremely low.

Another work is done by [23] entitled "A framework for the governance of cyber security in banking system in 2011; the purpose of this study was to identify the possible guidelines that can help in protecting the cyber problems by proposing an initial framework for the banking industries. The proposed framework was categorized into three levels which are strategic level, tactical operational level and technical level. Having a reputation for safeguarding information and the environment with in which it resides enhances an organization's ability to preserve and increase market share. The research shows that a comprehensive information security governance framework is highly needed for banking industries to satisfy the security need of business activities of the industries. The researcher also proposed adoption a better way of cyber security auditing frame work for the industry.

CHAPTER THREE - RESEARCH DESIGN AND METHODOLOGY

This chapter presents what research design and method was used to answer the research questions designed. Overview of the research methods: which includes 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? What instrument is used for data analysis?

3.1 Research Design

The research design was comprised 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

A mixed research method which combines both quantitative and qualitative method was employed to identify the existing cyber security audit system. The research begins with literature review by assessing previous researches conducted by different scholars and experts on cyber security in general and in the banking industry in particular in Ethiopia context. [40]. For the purpose of data collection, survey questionnaires and interview which are validated by selected expertise were employed to gathered relevant information that goes with the research study problems. Data were encoded and analyzed by using SPSS version 20 and MS-excel programs, and the findings were discussed and interpreted. Finally, a workable framework was being proposed, in order to mitigate the existing cyber security auditing problems.

3.2. Population and Sampling

According to the report from the National Bank of Ethiopia, there are about 20 banks found in Ethiopia owned by both Public and Private. All of these banks are currently engaged in financial transaction that includes, currency exchange, providing loan; depositing public moneys etc. These major activities are currently highly supported by information technologies. Among the existing banks the researcher used purposive sampling in order to select the banks.

Sampling is mainly based on ease of access to data and wiliness of banks and experts to provide relevant information that goes with the research problems.

Therefore, the selected data sources are both from private and government .Namely, Nib International bank, Bank of Abyssinia, Dashen Bank and Commercial Bank of Ethiopia (CBE). The criteria for the selection of the banks are based on the level of ICT usage, their willingness to provide data for the researcher. In the above banks, the primary data sources used in this study are IT 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 cyber security policy, standard and procedure documents were reviewed. In addition, standard compliance experts and financial audit professionals of bank and other institutions like Cyber security policy makers and regulatory body which were identified by Ethiopian government offices such as Information Network Security Agency (INSA), Ministry of Communication and Information Technology (MCIT) and National Bank of Ethiopia (NBE) were additional target respondents to the survey questions. In each of the selected banks there are about an average of 30-40 IT staff are there among this the researcher was interested to select only few of them based on lottery system with total of 100 and additional staff who have direct or indirect attachment with the cyber security system management of the organization and end service provider total of 100 finally total of two hundred questioners were distributed among all respondents. The research also includes interview session participants of 15 interviews who have deep experience and awareness in both management and use of cyber systems among the participants, IT experts, higher officials of the banks and relevant stake holders.

3.3. Data Collection

The intention with this thesis was in exploring, investigating, and understanding the current status of cyber security auditing in Ethiopia banking industries and proposing a workable cyber security auditing framework. Therefore, the samples have been selected, questionnaires were distributed and interviews were conducted, which are the characteristics of both quantitative and qualitative research methods. However, the fact that questionnaire is used as a tool for data collection dictates more of quantitative research methods though it is used in both qualitative and quantitative (i.e. Mixed research) methods. [40]

A questionnaire was developed based on the three categories such as Administrative, Technical, and Physical& environmental security. The questions items are open and closed on practices and status in Cyber security system management. The questioners were prepared and distributed to IT manager of the respective sampled Banks. The questionnaire developed had 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 cyber security, and the third section deals with the administrative aspect of cyber security. Were used to collect primary data from Ethiopia banks and other selected organizations for the study. The major focuses area includes security policies, organizational security, personnel security, physical and environmental security, communication and operations management, access control, system development and maintenance, and compliance. The response is used to see the existing practices , understand whether information systems users in organizations have awareness of cyber security , policies and procedures etc.[37], [19], [38]and Cyber security auditing readiness checklist for developing countries[38]. In addition interview were conducted for security and financial audit professionals based on the concept made by using Fredrik model of building a given framework , which was focused on three stages such us evaluation stage, formation stage and implementation stage. The result of interview has served as a guidance to propose a framework for the industry.

3.4 Data Analysis

After the data have been collected, the researcher turned to the task of analyzing them. After collect 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. The analysis of data requires a number of closely related operations such as establishment of categories, the application of these categories to row data through thematic coding, tabulation and then drawing statistical inferences. Thus, the researcher classified the row data into some purposeful and usable categories. Data collected using interview was analyzed inductively, building from particular to general themes by making interpretation of data for qualitative data. Percentage and graphical representation are used for quantitative data analysis, which resulted in

a flexible structure of report and data collected from qualitative aspect of the analyzed and interpreted using thematic coding [6].

3.5 Validation

Validations are done through user acceptance test hence the measurement or instrument is valid when it measures what it is expected to measure, and validity is concerned with the accuracy of the way of measurement [40]. Data gathering with the help of survey has its own threats to validity. For example the respondent may answer what he feels to answer rather than the actual fact exist [6], indicate that the best forms of protection against potential threats to questionnaire validity are careful attention to both the research process and questionnaire design. Validation involves the collection and analysis of data to test the accuracy of an instrument.

Therefore, both the questionnaire and the framework will be evaluated by designing relevant question which will be distributed among the senior IT officers and Experts in order to check for its validity and its workability.

CHAPTER FOUR - DATA PRESENTATION AND ANALYSIS

4.1 Introduction

Data analysis involves critical thinking. The data analysis is done after collecting all the data from the respondents. Thus, the analysis of the study follows the objective of the research. 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 the findings of the study and its interpretations are presented under each question items whereas suggestions are stated at the end of each security category. Moreover, the data were analyzed using statistical tools, such as graphs, tabulation and percentage using Microsoft Excel. Whereas, the data from interviews and observations were presented using thematic coding to assess the existing cyber security auditing framework for banking sector in Ethiopian. The responses obtained through questionnaires were integrated with interview results and physical observation in order to address the research questions.

4.2. Study Sample

The following banks were included in the study. These are: Commercial Bank of Ethiopia (CBE), Dashen Bank S.C. (DB), Abyssinia Bank S.C. (AB) and Nib International Bank S.C. (NIB). These banks were selected by purposive sampling method.

4.3 Finding and Discussion

The study used a self- completed questionnaire having close ended questions with likert scale format and Yes or No type. Before starting the main research, questionnaires were given to three staff members who are senior in bank security officers of two banks: Nib bank and Abyssinia bank as a means of pilot study. After accommodating recommendations from these groups of people, some questions were added and adjustments were made on some questions, to make them simple and understandable to all respondents. The final questionnaires were developed and personally distributed to all banks and then the student researcher has collected the filled questionnaires. Finally, the result of the readiness assessment helps to identify the real obstacles in the banking industry to implement cyber security auditing and in order to fill up the research gap in the country.

4.4. Findings

In this section, the results from data analysis are presented and addressing the main components of cyber security auditing framework 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. The result of the analysis is based on the responses obtained from four banks.

All control domains are categorized in to three based on the idea of [3]. The focus of cyber security evolved from physical security of computer centers to technical and then administrative cyber security.

4.5. Presentation and Analysis of Data

4.5.1. Respondents' Demographic Data

Overall 200 respondents participated in the survey. A total of 50 different kinds of questions were prepared to gather relevant information that goes with the basic research questions and problems to selected individuals and organization as indicated below refer table 4.1. As it is presented in table 4.1 the dominant number of respondents is male (76%), within the age limit of 20 – 30 (37.5%) and marital status of married (44.5%) and 50% not married. In addition more than 84.5% of them have educational level of first degree and second degree and above is 15.5%.

Table 4.1 Respondents Demographic Data

Variables	Proxies	Total Number	Percentage
sex	Male	152	76%
	Female	26	13%
	No response	22	11%
	Total	200	100%
Age	20-30	75	37.5%
	30-40	57	28.5%
	Above 40	48	24%
	No response	20	10%
	Total	200	100%
Marital Status	Married	89	44.5%
	Not Married	100	50%
	No Response	11	5%
	Total	200	100%
Educational level	First degree	169	84.5%
	Second degree& above	31	15.5%
	Total	200	100%

4.5.2. Current position

As shown in Figure 4.1 below the largest proportion of respondents (26.75%) are working as security expert followed by IT auditors (20.25%) and financial auditor (10%). The rest of the respondents are engaged as requirement risk analyst, database administrator, system administrator and no response that account for 13%, 12%, 14% and 4% respectively.

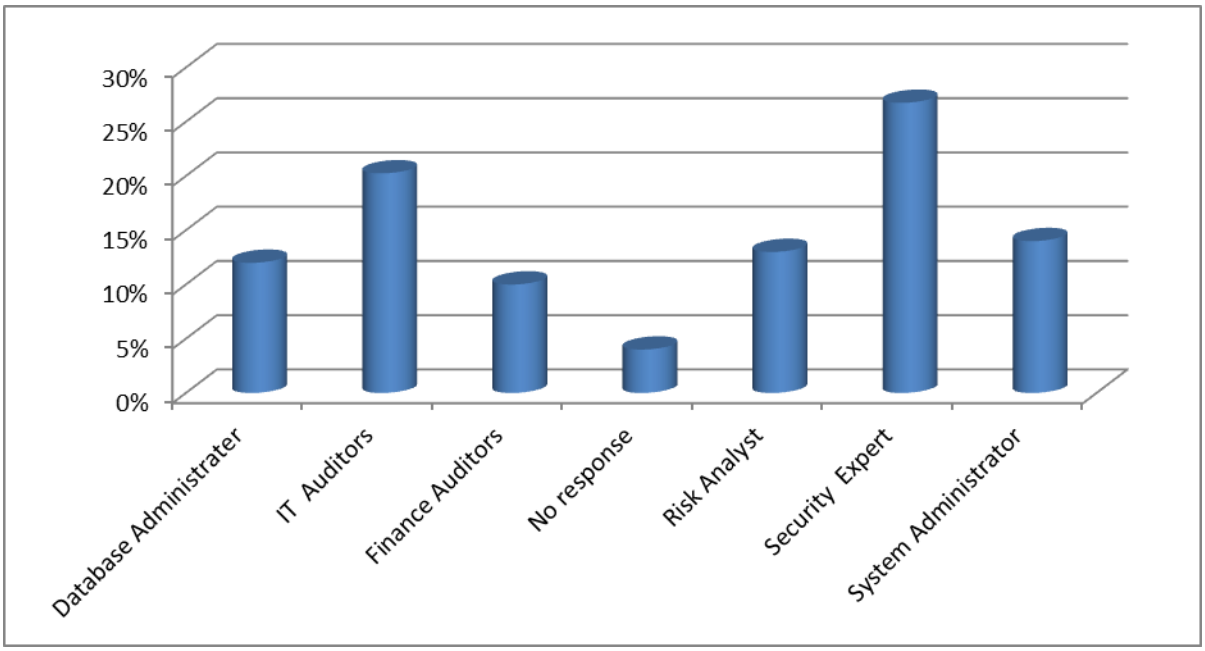

Figure 4.1: Position of respondents

4.5.3 Summary of Survey results from questionnaire

4.5.3.1 Administrative /Managerial Categories

Cyber security policy and standard

The organization's security policy is the set of laws, rules and practices that regulate how an organization manager protects and distributes resources to achieve specified security objectives [23]. These laws, rules, and practices must identify criteria for individual's authority, and many specify conditions under which individuals are permitted to exercise their authority. To be expressive, these laws, rules, and practices must provide individuals measurable ability to determine whether their actions violate or comply with the policy [14].

The selected banks were asked whether they have cyber security policies document & procedures, its implementation status, management support, update frequency, standards, an allocated annual budget and audited for cyber security. The result is summarized as shown below in figure 4.2, 4.3, 4.4, and 4.5 respectively.

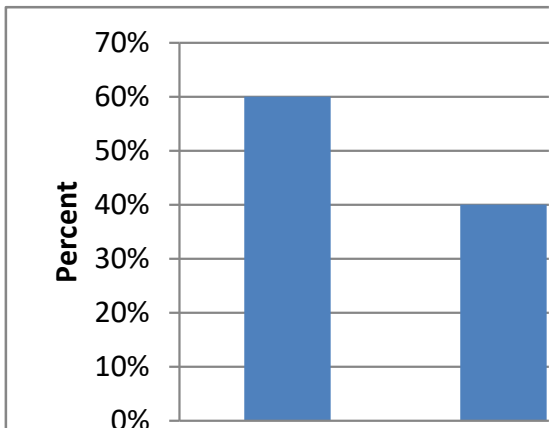

Figure 4.2 Cyber security policy and standard

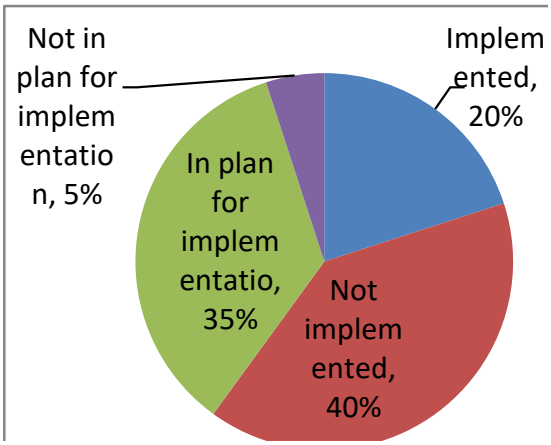

Figure 4.3 Cyber security policy implementation status

As shown in the figure 4.2 above, the findings from the survey shows that 40% of the surveyed banks don't have cyber security policy document while the rest 60% possesses the document which they cascaded and adopted from the national and international cyber security policy.

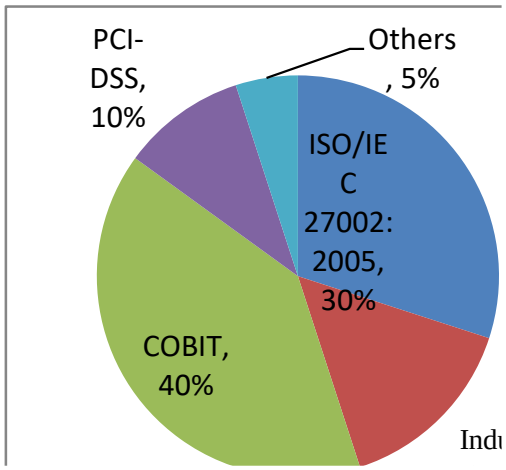

Figure 4.5 Standard usage information

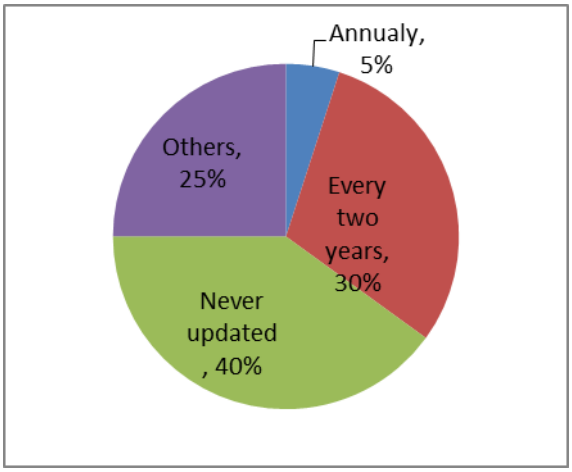

Figure 4.4 cyber security policy update

In the described figure 4-5 above, 40% of the surveyed banks COBIT, others use 30% ISO/IEC 27002:2005, PCI-DSS use 10% and 15% uses industry standards and 5% of those banks use other standards like in house developed. But when it comes to implementation, as shown figure 4-3 above, only 20% of the surveyed banks that have implemented their cyber security policy and 35% of surveyed banks that have the policy document are in plan stage of implementation. The rest 40% and 5% are undertaking the preparation and are planning to create the document and they are planning to implement in a very near future.

As shown in figure 4.4 above, 40% of the surveyed banks have never updated the security policy. This is mainly due to the fact that none of them is being fully implemented so far. 30% and 5% of those banks have updated every two years and annually respectively, where as other 25% of banks updated as required, there is no pre-defined plan for updating.

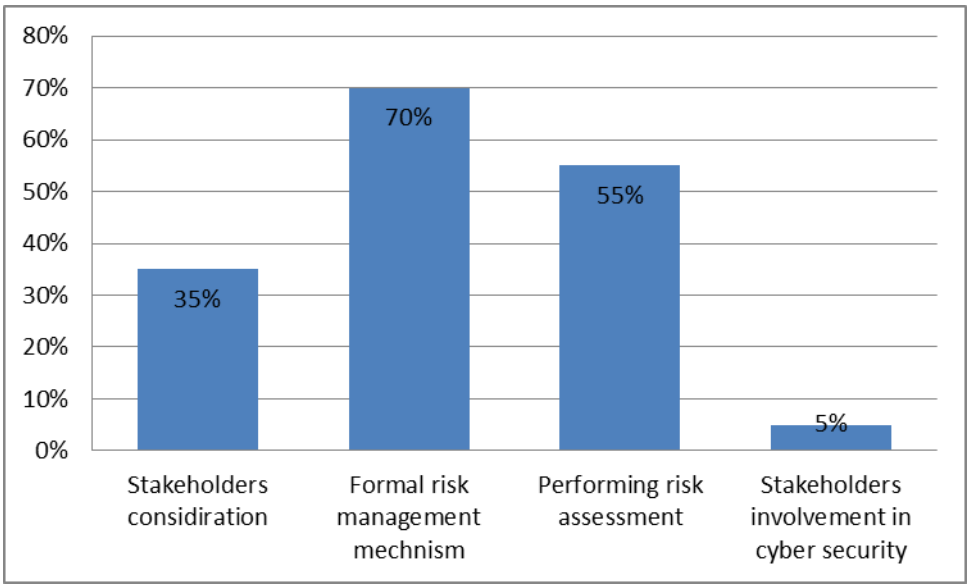

Figure 4.6 Stakeholders consideration, involvement, and risk assessment

As shown in figure 4.6 above, 35% 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 cyber security policy development. In addition, 5% 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 cyber security policy. 70% of the surveyed banks have considered the formal risk management mechanism. Only 55% of surveyed banks are performing risk assessment to identify security requirements prior to select best practices or controls whereas, 45% of banks did not perform risk assessment.

In the presented figure 4.7 below 85% of the surveyed banks have faced a problem of lack of experienced security staff on international standards, lack of local cyber security framework/standard, and 40% for annual budget for cyber security. As a result, these problems are hindered the implementation of cyber security system in their bank.

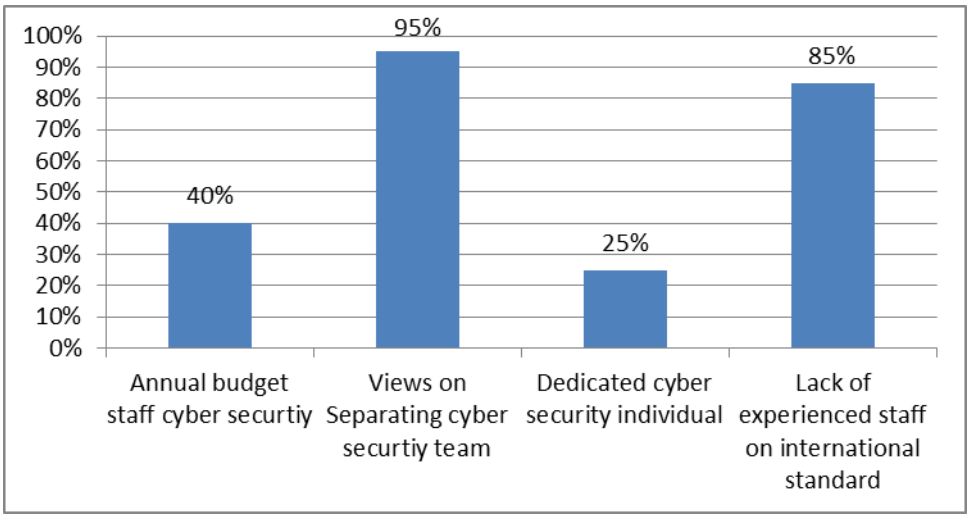

Figure 4.7 lack of experienced staff and budget, dedicated cyber security individual(s), annual budget for security awareness, and separating cyber security department.

As shown in figure 4.7 above, 25% of the banks have dedicated cyber security professionals with responsibility of assuring cyber security whereas 75% did not have dedicated expert. Only 40% of the banks have assigned annual budget for staff cyber security awareness program and technical training even though it is not enough whereas 60% they didn't allocate.

As shown in figure 4.7 above, 95% of those banks agreed on the idea of separating cyber security team (department or unit) from other IT staffs structurally under IT department.

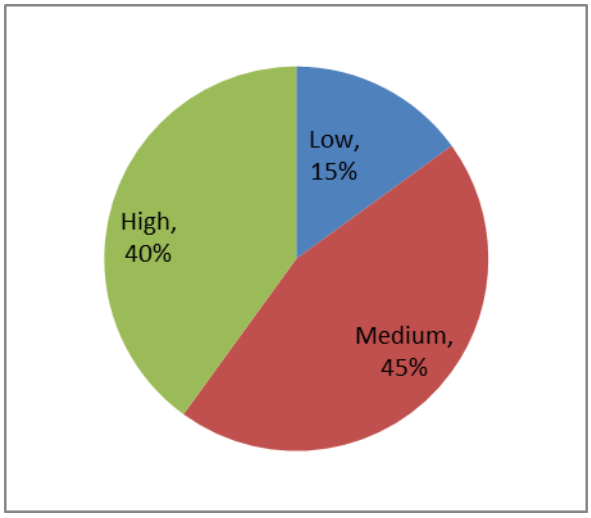

Figure 4.8 Management support

As shown in figure 4.8 above, in cyber security auditing process, surveyed banks has low, medium and high management support with 15% , 45% and 40% respectively.

2. Organizational Security

Organizational security has been seen from the perspective of existence of management consensus that ensures the management support to cyber security. The management of the organization follows authorization, organization, management and processes and has responsibilities to protect individual organization's inventory, information classification, third party access, security issues in contracts, and possibilities of finding specialists in the area etc. These were some of components of the organization cyber security that are addressed by the research.

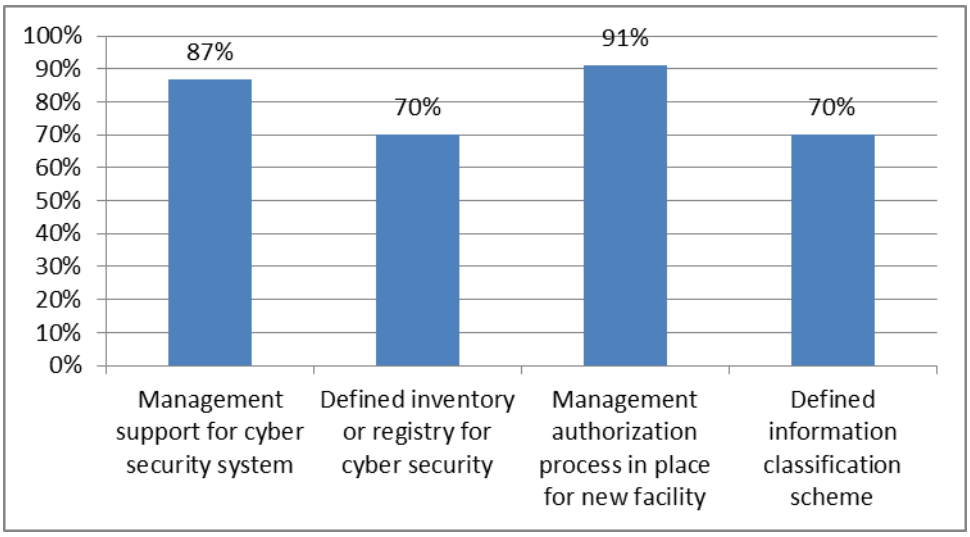

Figure 4.9.Management authorization and support for cyber security, define inventory for cyber security, and defined information scheme

As shown in the figure 4.9 above, 70% of the banks have defined inventory or registry with an accountability of assuring for cyber security system, where as 30% did not have defined inventory or registry. Only 70% of the banks have defined information classification scheme whereas 30% they did not defined. From the figure 4.9 above also, 87% of those banks agreed on the idea of management support for cyber security and also 91% management authorization process, for new information processing facilities including all hardware and software use.

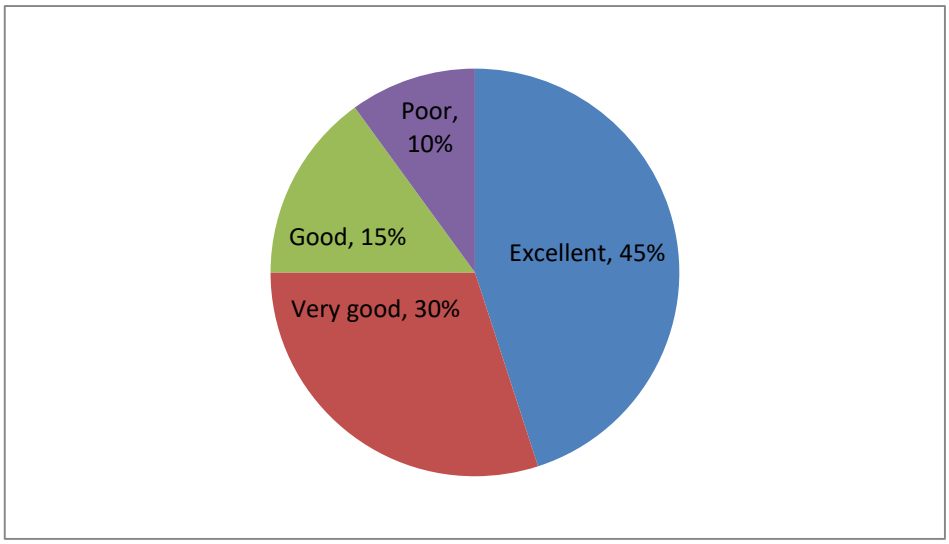

Figure 4.10 Management support

As depicted in figure 4.10 above, in cyber security system process, the surveyed banks has Poor, Good, Very good, and excellent management support to implement cyber security with 10%, 15%, 30% and 45% respectively.

3. Personnel Security

Personnel security has been seen from the perspectives of ensuring security of organization's information and IT resources as a result of employees and other third party access and use. Hiring a person working in the security area has its own procedure and requirement based on the level of their experts, experience they have and refer case personnel or organization they have.

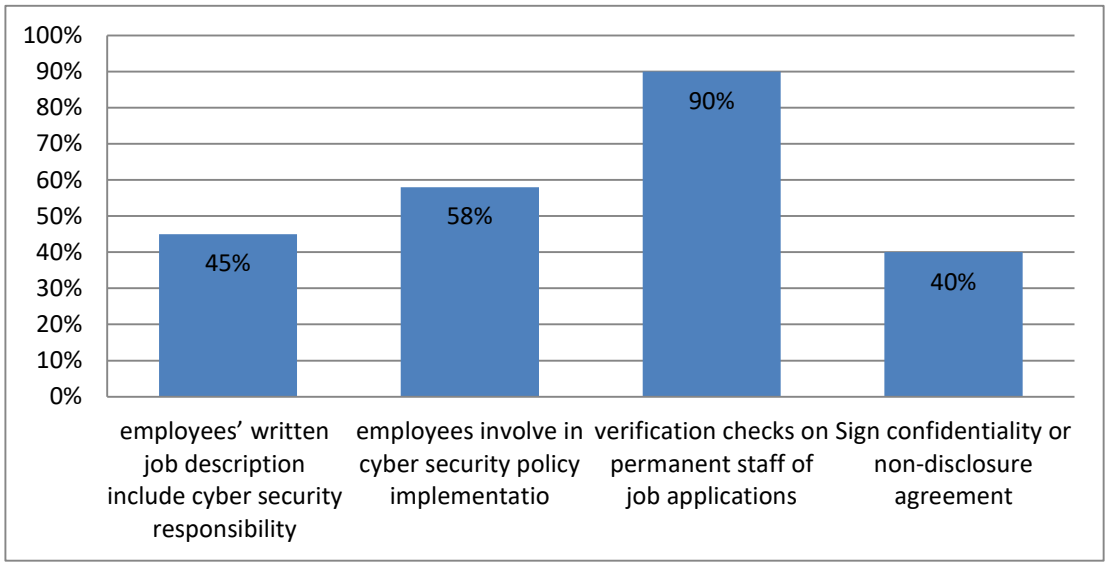

Figure 4.11cyber security responsibility is included in job description, policy, job applications, and cyber Security awareness for employees and third party

As shown in figure 4.11 above, employees' written job description includes responsibility for cyber security in 45% of the surveyed banks. And 58% of the banks invite employees to participate in the development of cyber security policies in order to encourage a sense of ownership. In addition, 40% of those banks have confidentiality or non-disclosure agreement with employees as a part of their initial terms and conditions of the employment and also 90% of surveyed banks has check on permanent employment staff of job applications.

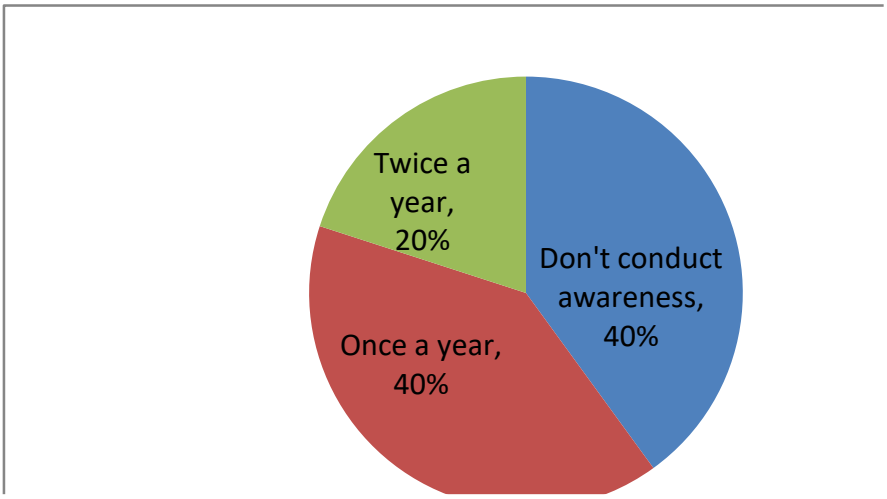

Figure 4.12 Employees and third parties awareness training

As shown in figure 4.12 above, in 40% of the banks surveyed, employees and third parties in banks didn't get training and updates on cyber security, while 40% replied that they do conduct training and awareness on cyber security once a year and 20% twice a year.

Figure 4.13 technical staff emerging technology awareness

As depicted in figure 4.13 above, technical staffs' awareness about emerging technologies and related control issues rated as Poor, Very good , Excellent and Good with 40%, 25% , 20 % and 15% of the surveyed banks respectively.

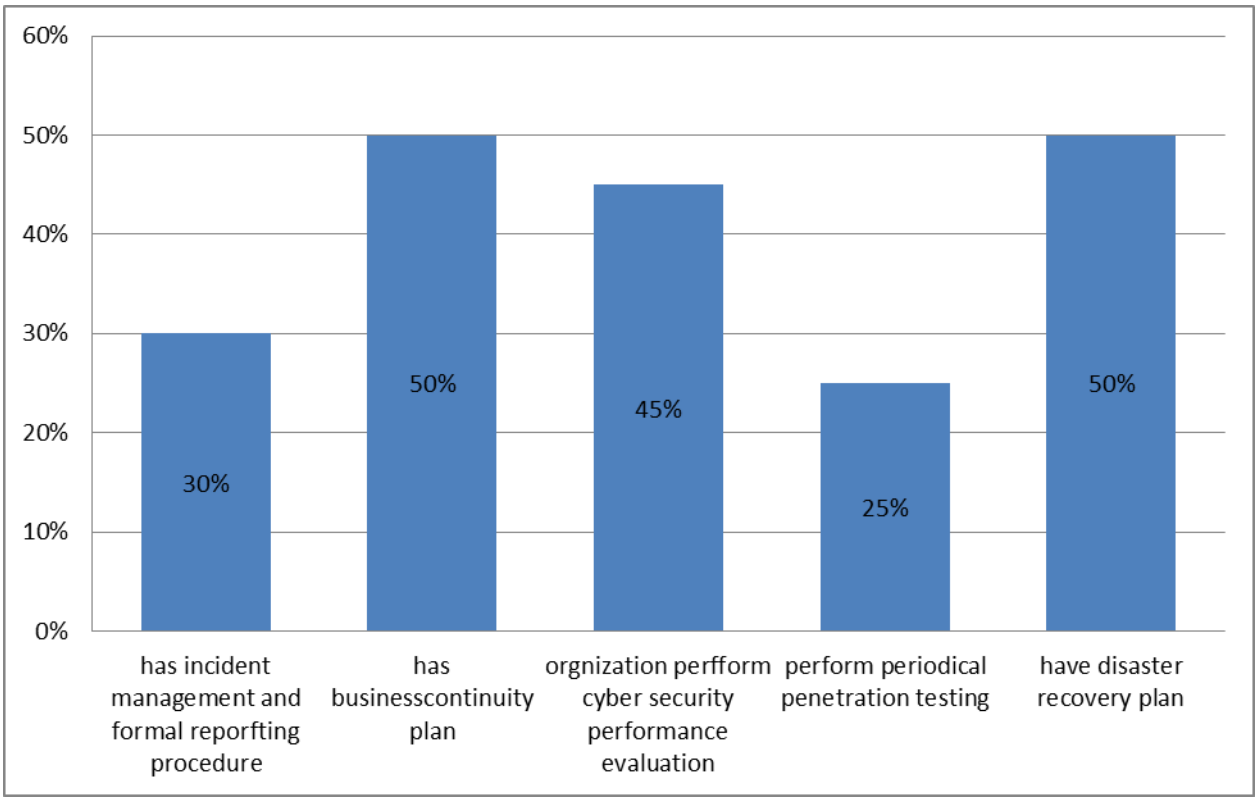

Figure 4.14 Incident management & formal reporting procedure, Business Continuity & disaster recovery plan, organization perform cyber security and Penetration testing

As indicated in figure 4.14 above, 30% of the surveyed banks have written incident management and formal reporting procedure to handle security incidents. But the remaining they don't have. In addition, 50% of the surveyed banks have an approved Business Continuity and Disaster Recovery plan. Only 25% of the surveyed banks perform periodical penetration testing and 45% of organization performs cyber security performance evaluation of their infrastructure.

4. Compliance

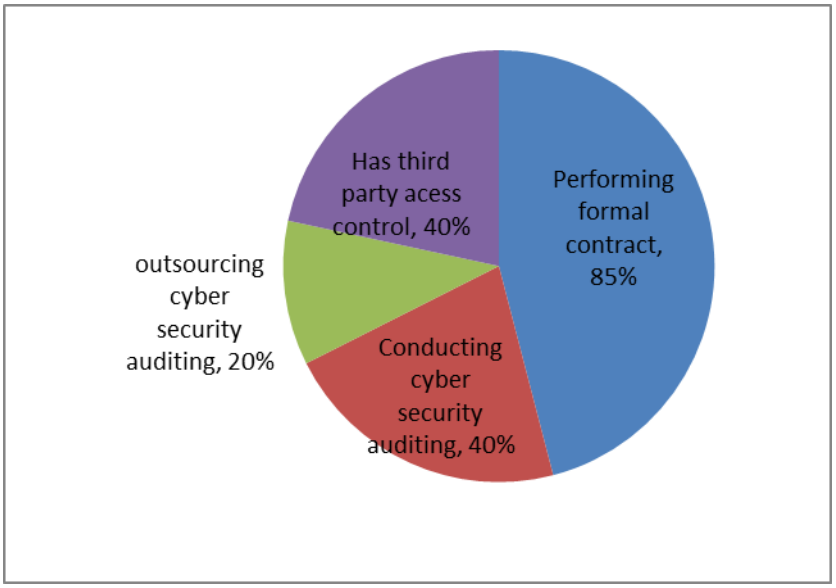

Figure 4.15 formal Contacts, auditing, outsource auditing and third party access control

As shown in figure 4.15 above, only 85% 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 conduct cyber security auditing at all. Only 40% of them did it. And 20% of the surveyed banks outsourcing their cyber Security audit to third party. In general, from the above diagrams, we can see that under administrative category, surveyed banks are weak in designing and implementing cyber security policies & procedures, standard usage, Stakeholders involvement, dedicated cyber security, management support, annual budget staff, personnel security, staff awareness training, performing periodical penetrating testing, incident management and compliance.

4.5.3.2. Technical (Operational Security)

Communication and Operation Management

The objective of this category is to ensure the correct and secure operation of information processing facilities. In this group the researcher has tried to see issues categorizing in five basic elements which are stated in figure 4.16 below.

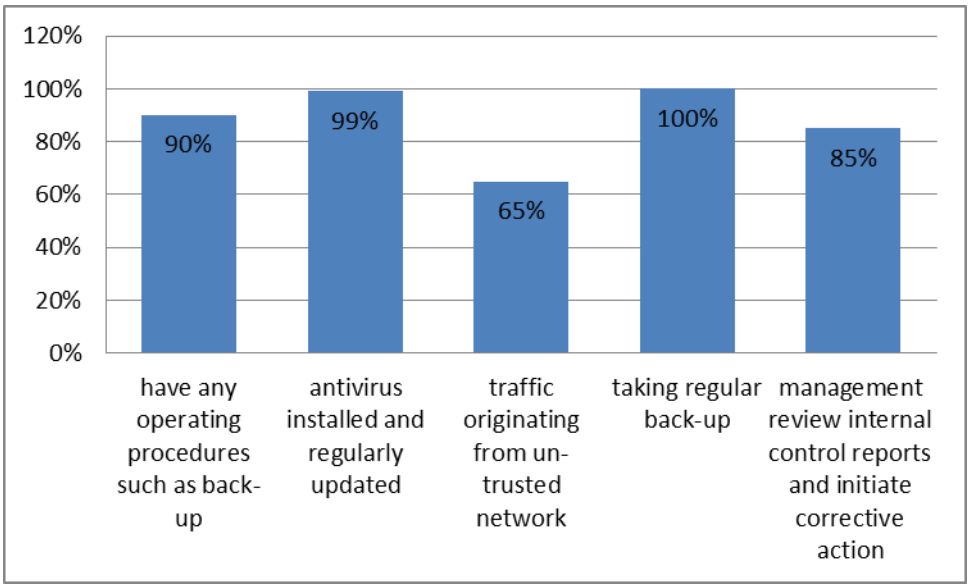

Figure 4.16 installed antivirus, web traffic filtering, management review, Operating procedures, and taking regular backup.

As shown from the figure above,90% of the surveyed banks have documented operating procedures such as back-up, and equipment maintenance and 100% of them takes daily back up of financial data and other like human resource data has taken on a weekly bases. Beside this 99% of the surveyed banks has installed and regularly update antivirus on computers that they possess. In addition to, 65% of them protect web traffics originating from untrusted network using firewall, and Web filters.

85% of surveyed banks have management review internal control reports and initiate corrective action where necessary.

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. In this group the researcher has tried to see issues by categorizing in to seven basic elements which are stated in the figure below.

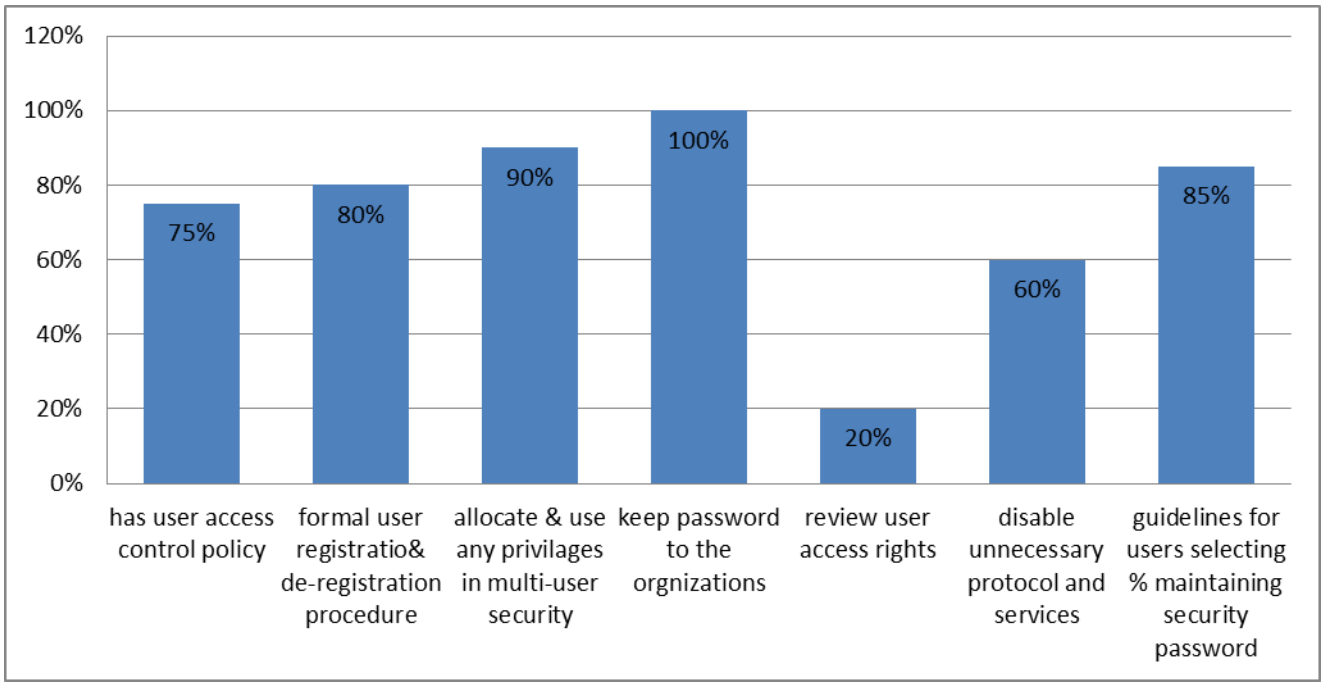

Figure 4.17 user access control, formal user registration& de-registration procedure, allocate & use any privileges, keep password of organization, reviewing user access rights, disable protocol, & guidelines for users

In the above figure 4.17, it shows that 100% of surveyed banks user sign a statement to keep password to the organization. In case of access right 90% to allocate and use any privileges in multi-user security and 60% of surveyed banks close or disable any unnecessary protocol and services.

In addition, 75% 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 the very critical resources of the server.

Only 20% of the surveyed banks have procedures to review access rights they grant to users as required and also 85% have guidelines for users in selecting and maintaining the security password of the organization.

System Development and Maintenance

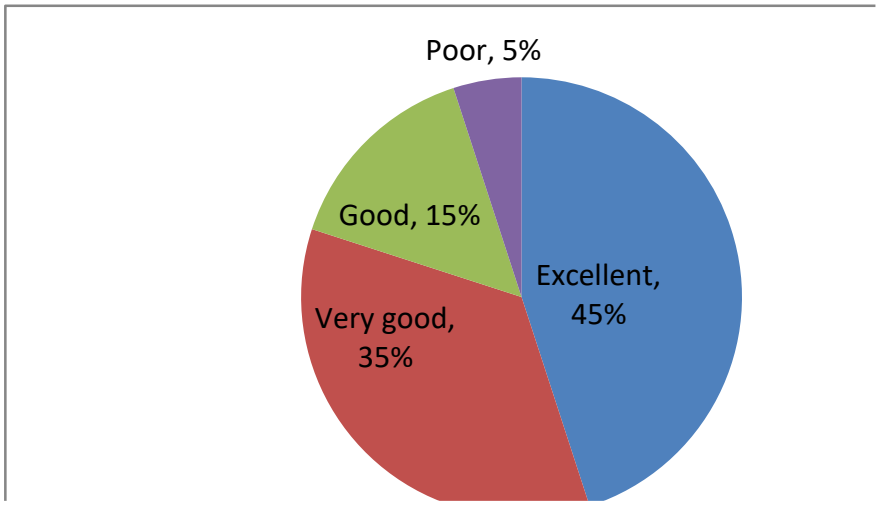

Figure 4.18 cyber security requirements study in system development process

As depicted in figure 4-18 above, a culture of conducting cyber security requirement study before system development in the organization rated as Excellent, Very good, Good and Poor, with 45%, 35% , 15 % and 5% of the surveyed banks respectively.

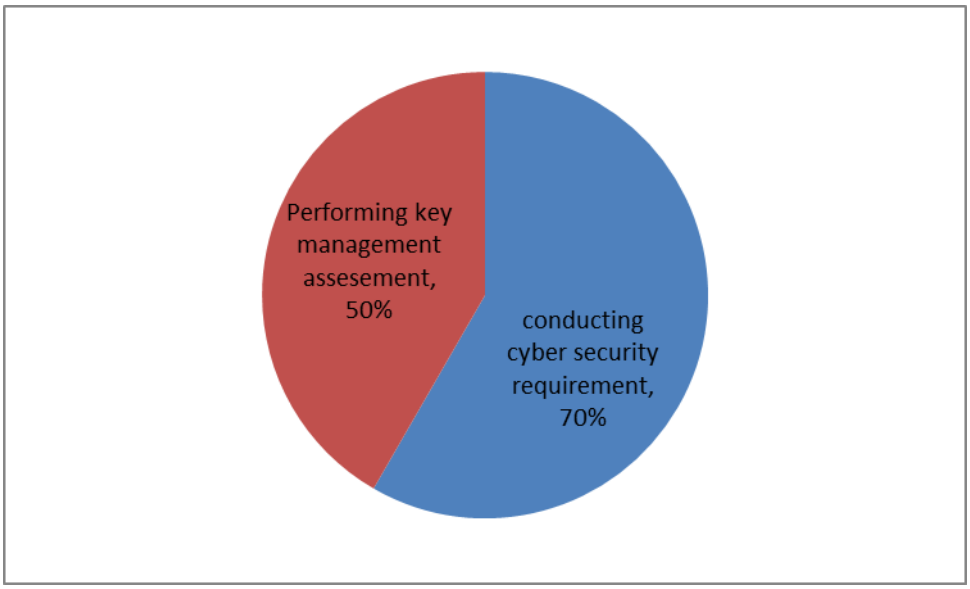

Figure 4-19 security requirements identification in system development process

In this category, as shown in figure 4-19 above, 50% of the surveyed banks execute business risk assessment to identify cyber security requirements prior their system development process. And 70% of these banks conduct cyber security system testing before production.

In general, the surveyed banks have medium technical security facilities to protect their sensitive and mission critical information even though they are so weak in performing key management assessment, and reviewing user access rights.

4.5.3.3. Physical and Environmental Security

Physical security is one of the parameters to measure how much organizations are ready to safeguard their assets from attack, damage or loss. This is the one where Ethiopian banking industries have better readiness (65.5%) of them have got better precautions either through traditional fencing or manned protection of the organization's territory while others are using CCTV cameras, cards and passwords controlled doors, etc. More than half banks data center, ATM card production center and disaster recovery sites have camera and door access control system. Personnel security guard, lock and safes are used to restrict access in some banks and/or branches. Least privilege and prohibiting third party from accessing to secure areas with the organizations are the methods that organizations are using to safeguard the secure access of third party.

Banks were asked whether they have physical and environmental security and the result is summarized as shown in figure 4-20,21,and 22 respectively below.

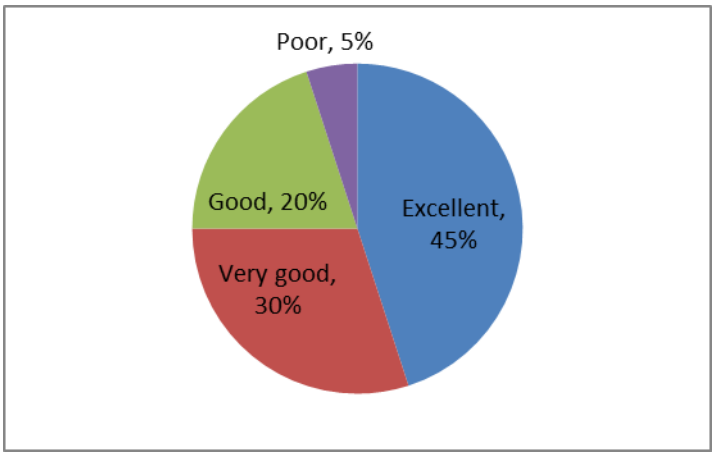

Figure 4.20 physical and logical securities

As shown in the figure above, the physical and logical security facility implemented, surveyed banks has Excellent, Very good, good and Poor to protect cyber security system of an organization with 45%, 30%, 20% and 5% respectively.

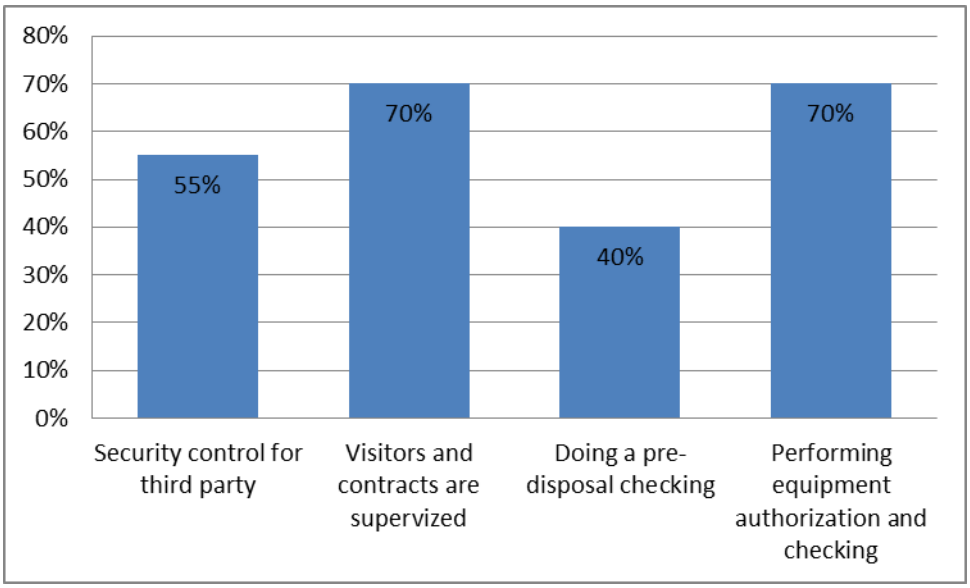

Figure 4.21 visitors & contractor's supervision, performing equipment pre-disposal authorization and checking.

As shown in figure 4-21 above, 30% of the banks surveyed do not supervise the visitors and contractors when they visiting the data center /server room while the rest 70% supervises them. 70% of the surveyed banks, authorization and checking occur on equipment entering or leaving your site while 30% 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.

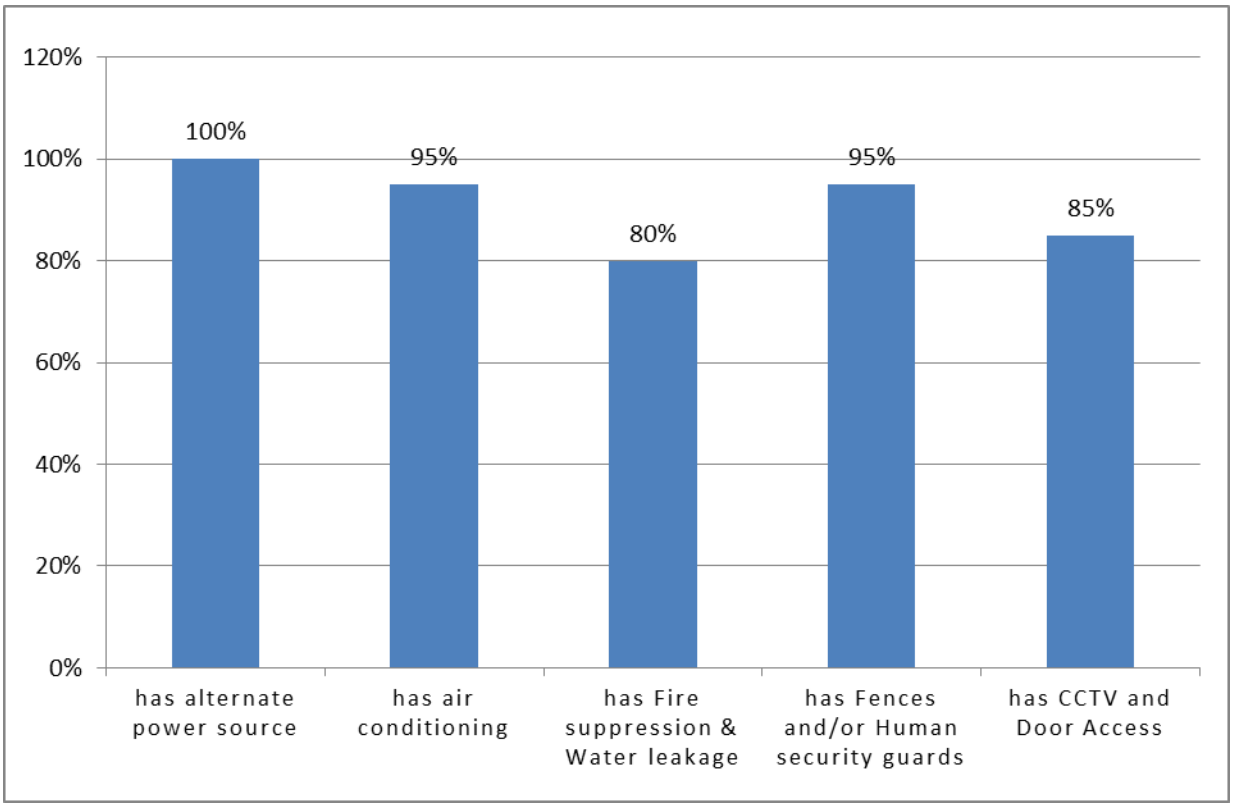

Figure 4-22: alternate power, AC, Fire extinguisher system, fences, and CCTV camera & door access system

As shown in figure 4-22, the finding from the survey shows that 20% of the banks surveyed don't have fire suppression, water leakage while the rest 80% possesses, and also 15% of the bank don't have door access control, and CCTV system, while the rest 85% possesses. But when it comes to alternate power supply (generator) 100%, Air Conditioning, and fence or security guard 95% all surveyed banks have employed.

In general, most selected banks 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.

4.6. Summary of the findings

Table 4.2 Summary of findings

Sno.	Thematic Areas	Practices and Challenges
1	Administrative /Managerial Categories	Lack of support from the top managing bodies of the banks
		Lack of skilled manpower in cyber security management and auditing in the areas of bank system
		Lack of training and awareness from management bodies ,of the banks
		Unable to allocate sufficient budgets for the bank system security enhancement mechanism
		Lack of domain experts.
		Poor awareness on cyber security issues for the staff of the bank
		Lack of guiding and controlling means so as to enhance security related problems
2.	Technical /Operational controls	Work overlap in IT department
		There is no a predefined security requirement identification methodology or model
		Poor knowledge on the international standards like ISO etc.
		In almost all banks there is licensed antivirus that can protect the system from viruses , well procedure and implementation of system back up ,
		Less attention and less controlling mechanism for managing traffic that come from untrusted sources
		Relatively better internal control report , Medium level of access control using passwords. Less skill in managing personal password.
3.	Physical and Environmental Controls	A better Power alternative sources in most banks , Better air conditioning for the data server ,
		Poor fire protection tools and mechanisms,
		Poor fences and CCTV cameras and Door accesses, for the data server and other bank cyber resources
		Poor equipment authorization and disposal mechanisms
		Better human security for the 3rd party gate

CHAPTER FIVE - THE PROPOSED CYBER SECURITYAUDITING FRAMEWORK

5.1. Introduction

In order to secure a bank's cyber resources the entities or organizations degree of interaction to the bank and business process cyber security risk level should be known prior to any business agreement to be made. Nowadays, cyber security is not only a technical issue, but also it is a management and organizational business success and failure issue for small scale and countries security issues at a large scale.

The literature review, questionnaire and interview findings and the researcher's findings and exposure shows that there is no local cyber security auditing framework that aid in development and implementation of cyber security framework to secure data in banking industry in Ethiopia.

Therefore, based on insights gained from the analysis of literature on various international frameworks such as ISO/IEC27k series, COBIT, PCI-DSS...etc., data analysis of interviews and questionnaire findings, and the student researcher exposure findings from different sources, cyber security audit framework has been proposed. The proposed CSA 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 CSAF process Model to identify a bank's cyber 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 its data flow among them. In CSAF process model it is employed to guide the bank's cyber 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.

Ethiopian banks 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 proposing a simple methods of cyber security control and management techniques.

5.2 CSA Framework Objectives:

The CSA framework objective mainly focuses on:

- Supporting the achievement and understanding of three cyber security objectives across banks: Confidentiality, Integrity and Availability of information.
- Providing a framework that assists banks to achieve cyber security auditing in banking industries.

5.3. The proposed Organizational Structure for IT Divisions in selected banks

The structure of IT divisions has a great contribution in cyber security management. All surveyed banks have agreed on this point and list out some limitation of generalist approach. For example, the generalist approach is inclined to attack, as a result employees' dissatisfaction, and high staff turnover is one of the causes.

Banks may have separate streams to manage their cyber resources in some form or other, such as hardware technical support, System and Application support, MIS, System Development and Customization, Data management System security, network infrastructure management and Data backups are among others. The primary responsibility of these groups is to manage their individual areas in terms of delivery, ensure compliance to the cyber security policies of the bank. The scope of this section is dealing how banks organizational structure for IT protects the organizational cyber resources.

Based on the student researcher's real world observation during the survey and expertise comment he has proposed a workable organizational structure for managing the CSRM indicated on figure 5.1. The bank's cyber security divisions itself might have two major division each having sub divisions, the director for cyber security resource audit and the director for cyber security resource managements. That further breakdown in to, Network infrastructure resource management and security, Application resource management and security, and Physical & Environmental resource management and security. 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.

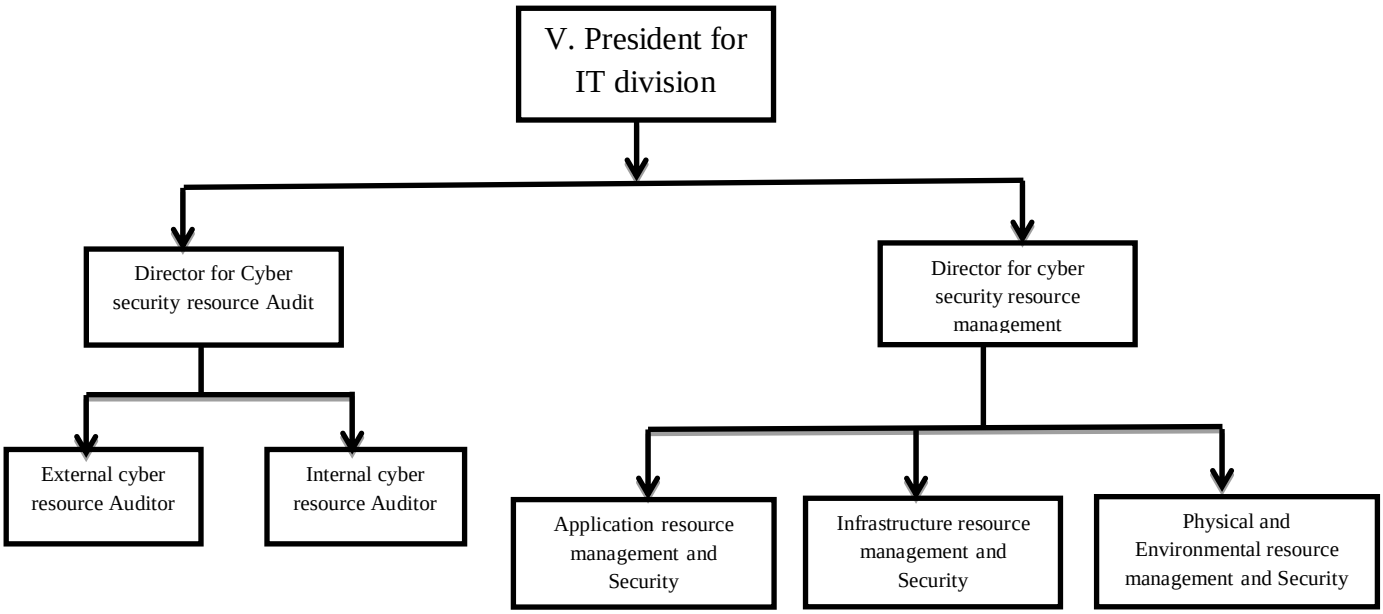

Figure 5-1 Organization Structure of CSRM

Director for cyber security resource audit and the director for cyber security resource management are directly reports to Vic president for IT division, in turn to higher officials or board. The two directorates of the IT divisions are responsible for creating secure operational and technical systems of the banks. Including the system administrator, data base administrator, web developer, technical supports etc. are also reports directly based on the divisions stated above.

5.4 Risk Assessment and Management Methodology

5.4.1 Risk Assessment

In identifying the banks risk it might want to adopt 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 cyber 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.

5.4.1.1 Cyber resource 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 about the criticality or value

of a resource. For example, for a physical resource (e.g. server) the value of the resource 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 or 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 [46]. 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 divided into the assets that support them, and so on.

The cyber resource identification process should at least identify:

- The bank's cyber resources 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, cyber resource utility programs, The existing network infrastructure, The communication links between the cyber resources systems and the outside world, The hardware in use (e.g. routers, firewalls, servers etc.).
- The owners of these resources
- Its value and sensitivity of cyber resources
- Threats to those resources
- Possible vulnerabilities exploited by the threats and implemented security management and control.
- Implemented security management and 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 and its systems process, who uses the data, and where it has to be stored [10].

5.4.1.2 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 risks such as:

- What was happened? What goes wrong?
- How could it happen?
- Why it is happened?
- Who is affected? What is affected?

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.

5.4.1.3 Risk Analysis

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

5.4.1.4 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.

5.4.2 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.

5.5 Major Components of Proposed CSAF

The outcome of the study is designing a conceptual framework which is more comprehensive cyber security auditing 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), CSRM (Cyber Security Resource Management) Process model, and a template.
- **Counter Measures** –policy, procedure, guideline, and controls

5.5.1 Requirement Identification Mechanism

The four surveyed banks' researched result indicates that there is no a predefined security requirement identification methodology or model. Currently, all surveyed banks employed the combination of lacks well organized knowledge, experienced of experts, Adoption of international policies, rules, regulations and recommendation. In addition, they also lack standards and clear steps in security requirement identification. Thus, the student researcher proposed the combination of three tools namely, ERM, CSRM process model, and template as a security requirement identification method.

5.5.1.1 Entity Relation 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 cyber security Process within a bank). In addition, this ERM is used to define data flow (in one way or two ways communication) between business entities [21]. Simply it helps to model the entities aspect of CSA Framework.

5.5.1.2 CSRM Process Model

After entities are identified using ER-model the cyber security resource management system process model which is developed by [9] is employed to identify potential risks and threats, designing a solution or select the counter measures, and to produce the implementation document. The cyber security resource management system process model describes the stages and the important activities involved in detail.

This model has three stages as stated by [9] such as Evaluation stage, Formation Stage and implementation stage (Figure 5-3).

5.5.1.3 Template

Cyber security resource management (CSRM) system 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.

5.6. The Design of Proposed CSA Framework for Banking Sector

The proposed CSA framework can be used as a starting point by banking sector to manage cyber security in developing and implementing CSAF to protect banking cyber resources 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 cyber security resource 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).

CSRM Framework has a great contribution in CSAF development even though it is a time consuming process, but it is a necessary perform secure operations of any cyber system. This paper describes the CSA Framework using cyber security resource management Process model, ER-model and template.

5.6.1. ERM- Different entities inter relationship to selected local banks of Ethiopian

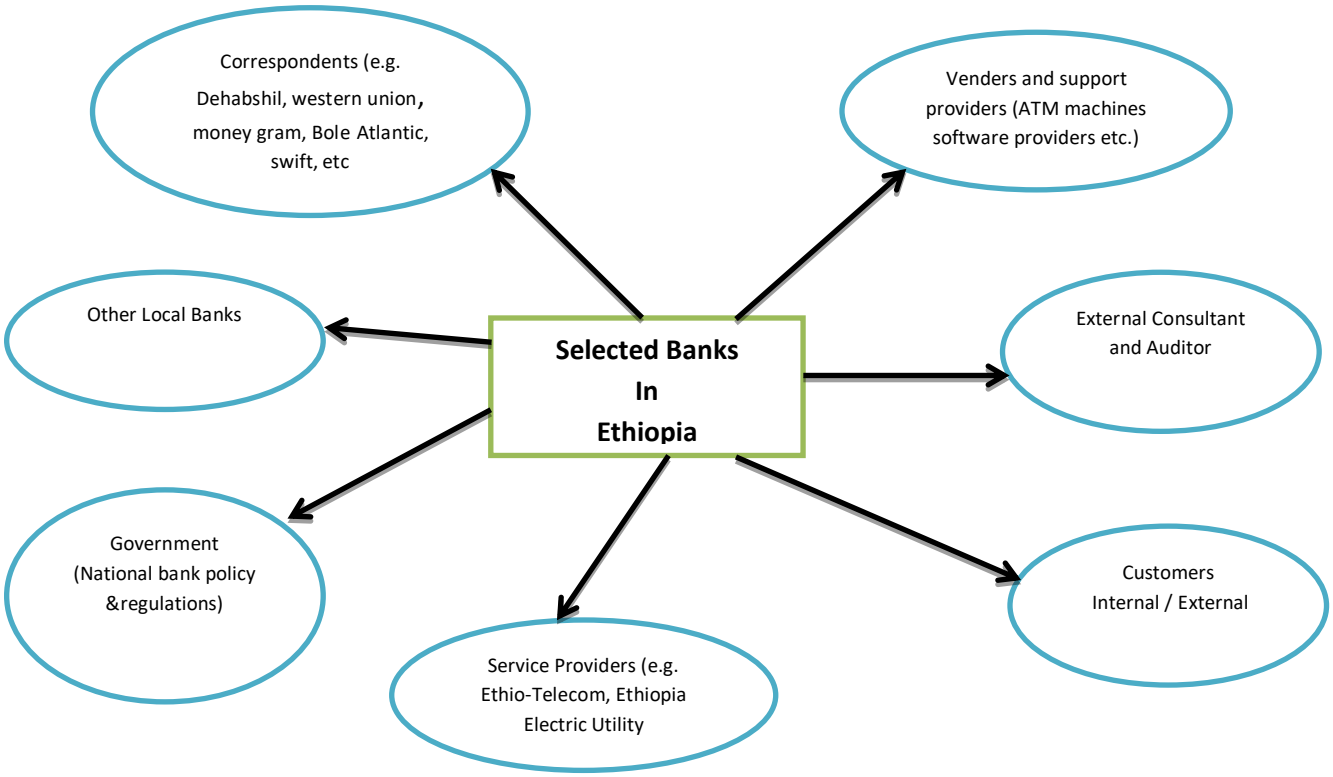

Figure 5-2 Different Entities Interacting selected banks

5.6.1.1 The description of each entity or "Responsible Parties"

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 cyber resources required for business process, level of interaction through the

communication channel. Data/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 cyber resource management by way of a contractual agreement that contains clauses requiring security of bank data and the regulation of access to a bank's cyber resources.
- ***Correspondent:*** A type of financial institutions which has a business objective and agreement with bank. For example, Dehabshiin, western union, Bole Atlantic, SWIFT, Money Gram, Express money...etc.
- ***Other Banks (Local Banks):*** A type of finical service providers which has a business objective and agreement with selected banks in Ethiopia. For example, the relation between CBE with NBE.
- ***Government:*** Bank regulations and policies are a form of government regulations which subjects 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 cyber resource management framework. These are:
  - An Internet Service Provider (also known as ethio-telecom) is companies that offer subscribe access to the internet or provide banks with an internet connection.
  - An Electric utility Service Provider is a corporation that offers electric power to banks.
- ***Customers:*** 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.
- ***Consultant*:** anyone who gives professional advice or services related to data management, information management to banks, IT infrastructure etc. for the bank 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 technologies.
- ***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.

5.6.2 Cyber Security Resource Management (CSRM) Process Model

This model has three stages .These is: evaluation, formation, implementation stages and feed back

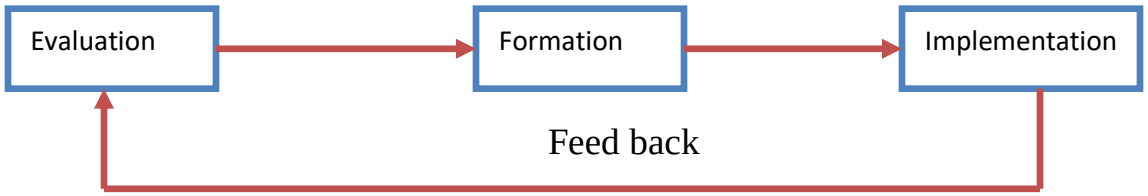

Figure 5.3 the model divides the CSRM processs into its sub-processes

- ***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 about cyber 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 cyber security.

- ***Formation 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 cyber security education and training to employees.
- ***Feedback:*** Once implemented, the cyber security auditing framework 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 cyber 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, cyber security management system

development team of a bank needs to gather some data (table 5-1). That is, data gathering based on business objective and security strategies of the bank. There should be pre-evaluation task.

Parameters that are considered in the template are:

- ***Description***: tells the involved entities in the given relationship or business process.
- ***Channel***: means of communication between selected Banks and any entities or division 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 CSRM process model
- ***Outputs***: the result of each stage after processing the inputs.

Table 5-1 Template for Evaluation stage

Description	Channels (Means of communication)	Inputs	Procedures	Out put
A business relationship between Banks and venders	paper, email, electronically	- Business strategy - IT strategy - business Process knowledge – cyber resource -Public Financial institutions Agency's orders -Directives issued by the NBE -Policies and procedures of the bank -Directives issued by the bank -National cyber Security Policy	-Identify critical & non critical business processes - Identify cyber resource 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. - Vulnerability scanner	Assessment report such as: - Risk and Gap analysis reports -Technical report on vulnerabilities -Top management awareness - Understanding of how cyber security relates to business

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

B. Formation stage

The goal of the formation stage is to design a technical and organizational infrastructure for cyber security that suits the business. Such infrastructure is documented as cyber 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 cyber securely.

Table 5-2 Template for Formation stage

Inputs	Procedures	Out Puts
- All outputs from the evaluation stage - Cultural knowledge - Business- and IT knowledge - Countermeasure / control knowledge (efficiency, cost, etc.) - Best practice - Legal requirements - Current CSRM if any or any existing rules	- Identify internal requirements on the CSRM - Design and document technical countermeasures - Write policy and procedures (CSRM) **Supports** - cyber security standards - Electronic forum - CSRM templates if any	- cyber security policy - cyber security management system - counter measure design document - Partial Top Management awareness

C. Implementation stage

The goal of the implementation stage is to take the CSRM documents, including also the technical controls, from the design document to reality.

Table 5-3 Templates for Implementation

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

The rules in the CSRM 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 CSRM. Also, all the IT-related solutions have to be installed or (re-configured).

Cyber security has to be marketed so that the bank accepts adherence to the rules laid out in the CSRM. 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 CSRM. 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 advantage and disadvantages of the feedback and take action.

5.6.3. Within selected Banks

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.

Cyber security resource management shall be accepted as an integral part of bank governance, in turn associates with IT /cyber security resource management. Cyber 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 data.

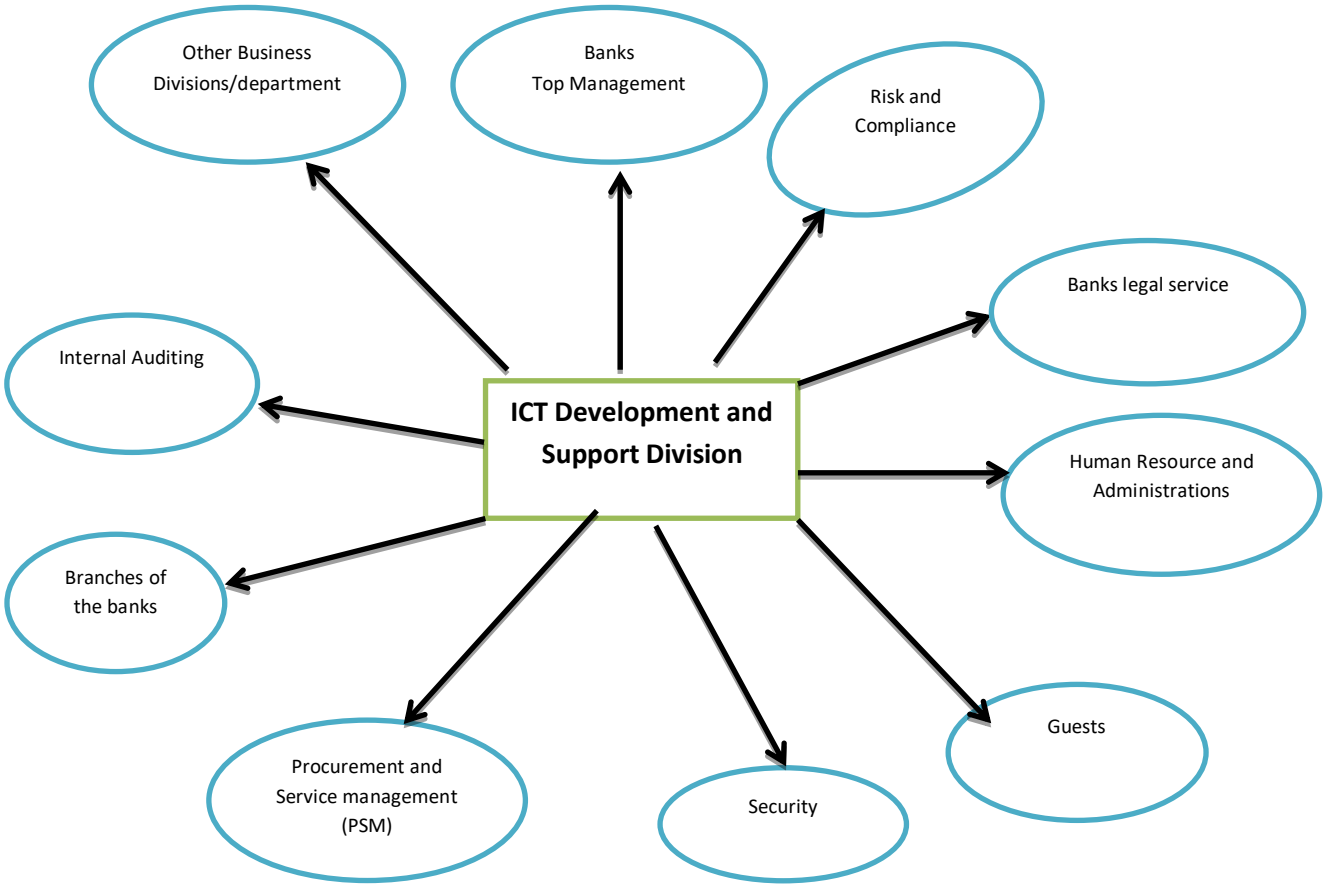

Figure 5-4 Internal entities relationship to cyber security process

5.6.3.1 Description of Stakeholders /Entities within Selected Banks

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

- ***Bank's Top Management (BTM)*:** it includes senior executive management members. BTM is one of the key administrators of a financial institution. This top management performs 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 data from the system which is owned by IT Directorate division.
- ***ICT Development and support Process:*** Ensures the overall smooth operation of the cyber security resource management 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:*** 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 data from the system which is managed by cyber security resource management (CSRM) department since it is the owner of the cyber system.
- ***Bank's Internal Audit Process:*** The Internal Audit Process (IAP) bears primary responsibility for audits. IAP conducts audits in accordance with the banks internal polices and 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 and Administration:*** 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:*** This has a mandate for assuring physical security of the bank and cleaning the server room/ data center and disaster recovery and the whole compound by large.

5.7 CSRM Framework Components

It is noted that none of the frameworks /standards cover all cyber security resource management components; some of the framework such as PCI-DSS 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 data's.

According to [23] State that although it is often speaks of "best practice" in connection with data security, in practice there is no standard that completely regulates all of the aspects of cyber security and can fulfill the needs of individual banks to the same degree. The reasons why there cannot be universally correct cyber 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 cyber security for the achievement of particular business objectives and a correspondingly different willingness to pay for it.

Bank cyber security resource management should have its own place within the framework of bank governance, beside cyber resource governance and risk management. The effectiveness of CSRM 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 CSRM 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.

Adopting to the cyber 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 CSRM, the CSRM 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

Therefore the newly proposed frame will have fundamental elements that should all banks cyber security resources could be controlled and managed, but there might be variations in the detail components of the cyber security controlling and managing element among different banks which will be cover in the proposed framework.

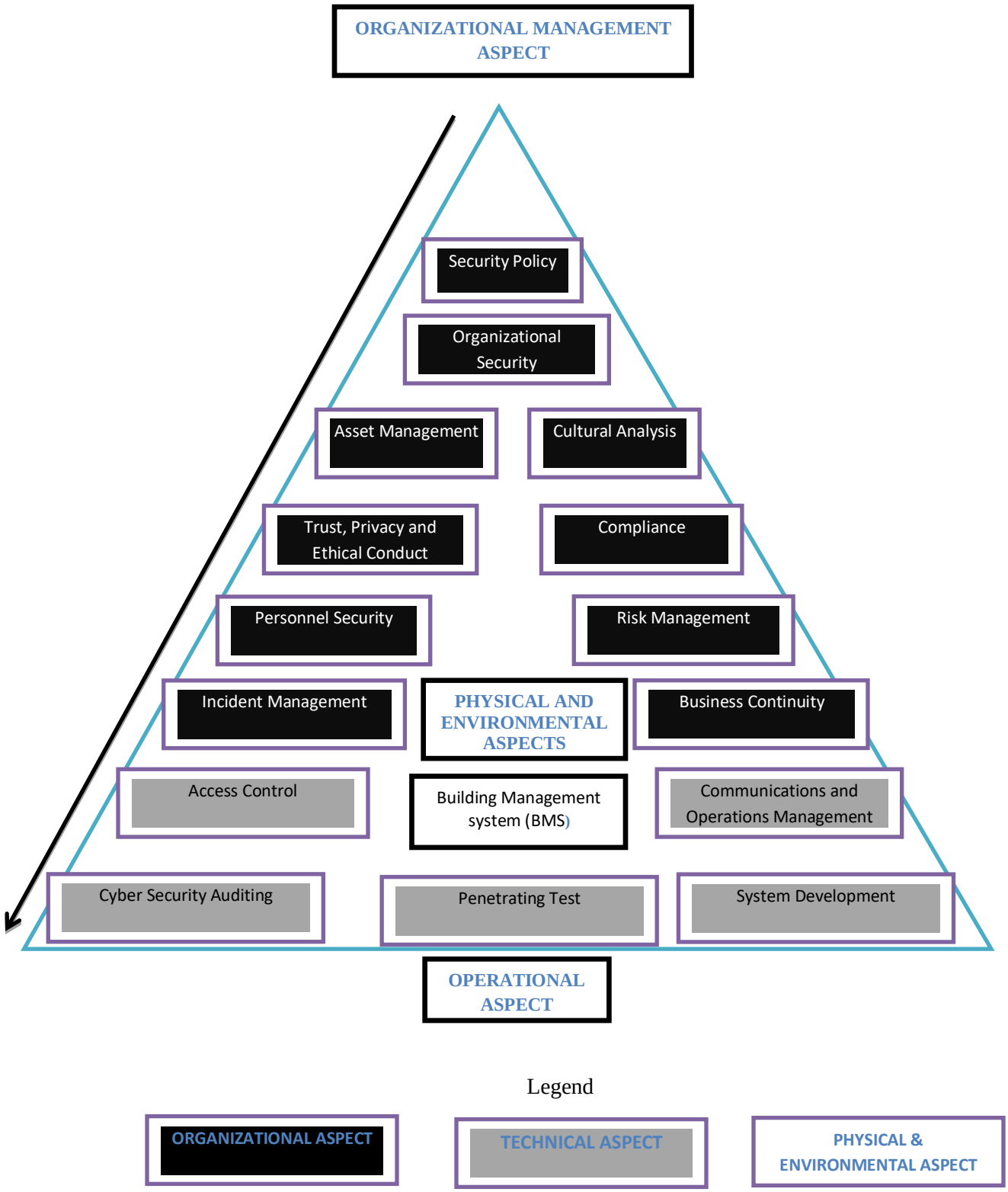

Figure 5.5 Proposed CSAF

Based on the literature review, questionnaires and interview findings 16 main control objects are identified the sources for such controls are derived from international standards, Literatures and challenges from the real world during the survey. All these 16 components or control objects are summarized using organizational structure for easy understanding as shown in figure 5-5 above.

These components are further categorized into three major groups for easy of understanding such as Administrative, Physical & environmental, and Technical & operational issues.

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. Cyber Security Incident Management:*** To ensure cyber security events and weaknesses associated with cyber 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 cyber 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 set by the banks policy and regulations.
- ***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. A cyber security policy must be developed which reflects bank's objectives, management support and commitment, and core values gives to technological advancements.
- ***A8. Organizing Cyber Security*** – Management must establish a framework to initiate and control the implementation of cyber security. Cyber security must extend to external parties.
- ***A9. Cultural analysis:*** To keep and understand the society where the business runs in and be able to obey and protect the resources from misuse.
- ***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 cyber resource.

C. Technical /Logical security- Security Control Objects

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

5.7.1 List of Recommended Cyber security Policies

When implementing the cyber security framework the combination of the administrative, technical, and physical & environmental 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 cyber 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 cyber Security Policy of a bank that requires policy.

- ***Statement of authority and scope***- Defines who in bank sponsors the cyber 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.
- ***Cyber resource Audit policy***-Defines audit policies to ensure the integrity of cyber and resources. This includes a process to investigate incidents, ensure conformance to security policies, and monitor user and system activity where appropriate
- ***Data 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 "cyber security team" to identify, assess, and remediate risks to the cyber resource 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 cyber information sent or received by email should be retained and for how long
- ***Spam policy-***Defines how spam should be reported and treated.
- ***Cyber resource 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 Ethiopian Electric utility 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

5.8. Validation of CSAF

Introduction

It describes the validation of cyber security auditing framework for banking sector in Ethiopia. Firstly, it introduces why the researcher designed the framework and what the researchers expect to receive as the results from the case study. Secondly, it describes the participants and gives the reasons why they were selected. The researcher continue and report how it is carried out the study and summarize the interviews. Finally, the researcher has provided the results of the case study.

5.8.1. Introduction to an integrated test framework

The framework contributes to the security of bank system in general and its Auditing environment with the means to evaluate how safely the cyber resources are controlled. To confirm the workability of the security auditing framework an evaluation is needed for its implementation of the framework, we carried out a case study among four banks. The purpose of the study was to understand whether the framework fit for use and to find out what should be done to improve the framework's workability

5.8.2. Participant Selection:

Four security professionals were contacted and asked to evaluate the newly proposed framework versus their own banks security tasks and activities. The limitation of the participants to four professional were mainly due to the limited number of banks professionals who are currently practicing in the bank system security. The researcher wanted to carry out a small proof-of-concept to evaluate the framework, not to make a full research on the matter. The participants were selected from four banks, in order to confirm how the company specific security activities are performed.

5.8.3 Validation Framework Workability Interviews

The study gathered responses to the questionnaire addressing the workability of the framework

The researcher used personal approach and performed interviews with the respondents. This

Provided closer feedback and allowed us to ask additional specifying questions when the answers were vague or superficial. Firstly, we introduced to the participants the purpose of the framework and also

explained based on theoretical studies which were later confirmed by performing survey among the selected banks. The survey results were analyzed, for all security frameworks based on the following interview questions.

- How easy is the framework to learn?
- How efficient is it for frequent use?
- How easy is it to remember the activities in each phase of the framework?
- How satisfied are you with the framework?
- How easy it is to understand the benefits of the framework?

The first two interviews revealed that the guideline requires a change. We improved the framework guideline thus making it easier to understand. After that, we proceeded with next respondents. The interviews with the respondents lasted on an average an hour by raising relevant comments by the respondents. Three of the interviews were recorded using phone while one respondent asked us only to make footnotes. The goal of the interviews was to understand whether improvements should be made to the framework and to get feedback on the workability.

5.8.4 Results of the Case Study

Each of the study participants was asked to give feedback on the framework usability and to rate it on a scale of 1 (lowest) to 5 (highest). We provide the results in Table 5.8 below

Table 5.4 Response to validation

Questionnaires	Respondent I	Respondent II	Respondent III
How easy is the framework to learn?			
How efficient is it frame work to use?			
How easy is it to remember the activities in its component			
How satisfied are you with the framework?			
How easy it is to understand the benefits of the framework?			

The first response about the ease of learning is lower than the others, since improvements were made to the framework guideline based on the interviews. The rest of the survey does not have outstanding differences.

- **How easy is the framework to learn?**

After applying improvements to the guideline, all respondents considered the framework easy to learn. People understood the workflow how to use the framework. They also implied that there are clear activities are mentioned in each of the phases. Respondents recommended creating the evaluation framework a good approach in understanding.

- **· How efficient is it framework to use?**

The respondents understood that for frequent use, professionals were responded that it would only have use the frame work frequently for sometimes then it is easy to remember. As such, most respondents found that the framework is rather efficient for use.

- **· How easy it is to remember the activities in its components framework?**

Most of the interviewees told that the activities in each of the phase are easy to remember. They said that activities in the phases are logical and quickly followed. One respondent did suggest shortening the activity.

- **How satisfied are you with the framework?**

This question turned out to be the hardest to answer. The participants had never used a framework for evaluating the security issues; it was new experience for them. While they did not say they were not satisfied with the framework, they were also reluctant to confirm, that it met their expectations. There was one exception, one of the professional believed, that evaluating framework needs sufficient time.

- **How easy it is to understand the benefits of the framework?**

All respondents understood clearly the benefits of the framework mitigation of the subjectivity of evaluation by using an evaluation framework based on structured approach. Similar to the previous question, there was outstanding respondent who strongly believed that the framework would not be beneficial for the bank system. Despite the outlying result, majority of the interviewees agreed that the benefits are rather easy to understand. Finally, respondents were asked to bring out the best aspect of the framework. Three interviewees told that they got a clear understanding on how much it meets with banks expectations. The other one agreed that the framework is excellent for frequent use and saves time.

5.8.5 Threats to Validity

We have applied the guidelines (e.g. personal interviews, objective questions, addressing potential risks to validity) suggested by [37] to minimize the threats to the validity of our case study. However there are still few which should paid attention be to when reviewing the results. The first and probably

the biggest threat, is the number of participants in the case study. We asked 4 professional to evaluate our framework. The number of the participants was kept low due to the lack of professional and willing to respond the questionnaire. For future work, further analysis should be carried out by including more respondents to the evaluation framework's usability case study. Another aspect which should be mentioned is that the framework validation focused only on the usability and did not address the completeness of the security framework. To address this risk additional research should be carried out to confirm if all required test features have been included to the evaluation framework. Finally, a threat to the validity of the case study comes from not confirming the correctness of the evaluation framework. We have not investigated if the framework will produce the same results for different respondent groups who evaluate the same test frame work with other security system evaluation framework. Our focus was only on the framework usability and thus, the correctness is subject for future work.

5.8.6 Summary of the Framework Validation

The researchers carried out a case study to investigate the usability of the cyber security framework evaluation. The study involved 4 practitioners and they were asked to evaluate their banks system based on the proposed framework .The result of the evaluation confirms that the framework is easy to learn, efficient for frequent use and fit for purpose. There was one respondent, who was doubtful of the framework suitability for the task, In addition the student researcher has made an improvement based on the comments given by the professional in the areas of its guideline to follow a stepwise approach in which the In conclusion, the strongest aspects of the cyber security frame Auditing framework are efficient and it reduces some of the risk in the area.

CHAPTER SIX - CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORKS

This chapter presents recommendations for the banking industry in general and particularly for Ethiopia banking industry; based on conclusions of the research described in the thesis, the objectives of the research, outlined in chapter one are reviewed and addressed their achievement. Finally, proposals for future work are suggested.

6.1. CONCLUSIONS

In today's technological and social environment, cyber security is a very important part of a banking system. Business partners, suppliers, customers, and vendors require high cyber security from one to another, particularly when providing mutual network and data & 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.

The general objective of this research was to propose generic cyber security auditing framework for banking sector in Ethiopia. To achieve this objective, the researcher selected Ethiopia banking sector to understand the current cyber security auditing by investigating the readiness situation and identify factors that influence security audit implementation on the industry. After sharing experiences and knowledge from the survey study, then put it in to the existing knowledge on the subject matter, which identified from document analysis and literature reviews. Finally, a new framework has been developed to help the banking industry for exercising cyber security audit activity. The empirical study was done through mixed research method; questionnaire designed was based on ISO, NIST, and ICT security readiness checklist based on twelve minimum security requirements and data was conducted with professionals, having good experience on the subject, by using Fredric framework model. Therefore, based on the researches finding, Ethiopia banking industries are at low level of readiness. The capability to conduct cyber security audit partly depends on the existence of policies, procedures and processes, which the majority of Ethiopia banking industries are lacking. The existence trained man power in the area, consulting firms specialized in cyber security auditing, IT staffs readiness, etc. also have low readiness in the country. The study shows it is in adequate. To solve the existing situation we recommend having cyber security auditing framework. It enables organizations to have standardized approach of addressing cyber security auditing by realizing the requirements: cyber

security polices, standards, procedure and processes in the different security management domains. Therefore, the research proposes a workable cyber security auditing framework that contributes for the industry as a starting point for cyber security auditing.

6.2. Recommendations

1. The framework can be used as an initial effort for practitioners in the banking industry to manage their cyber security. The results of the research also imply the need for further researches to make the framework more compressive and useful.
2. The framework should also be inclusive through rigorous testing to minimize the limitation of the framework
3. The framework should also be strong through upgrading it elements in different approaches
4. There need continues follow up for its validation as per the dynamic cyber security challenges of the real-world.
5. The Organizational management aspect, operational aspects and the physical and environmental aspect should fit to the best level of the current challenge, mitigation strategies.
6. Beside the above listed recommendation there needs cyber security training for all employees in organization is important;
7. Frequent workshops or seminars should be organized on cyber security on top of training;
8. Government and other responsible organizations need to formulate ethical hackers team and cyber security audit firms by encouraging with some special benefit (like tax shield, office facility) up until the proper awareness about cyber security audit made to people and organizations in the country;
9. Need to formulate security professions association for challenging things in group:
10. Encourage researchers to work more on security and related areas to develop more personnel in the area.
11. A national or regulatory bodies that manages and leads the country's cyber security needs to formulate a program and give training to different organizations in country about the use of cyber security and policies;
12. Laws and policies must define what is right what is wrong as well as what penalties are put in place for violating security policy and prepare legal framework for security audit;

6.3. Future Works

Generally, cyber security is still a very complex field of research, with a lot of unexplored facts in the areas. Therefore, we recommend that, the subject needs more researches to explore essentials. But particularly, as it is stated on scope and limitation section, the scope of this research was proposing cyber security audit framework only for banking sectors. However, as a future work researchers need to address the following:

1. The situation in other financial institutions , governmental organizations and/or generally designs international or national approach that could benefit general public, organizations and individuals help to solve the real cyber security problem.
2. Although, in the banking sector, quality of services and technological adoption is their major focus but, there is a trade-off strong security implementation and internal control with their focus. Therefore, it has to be considering for future research.
3. Enhancing the same research by considering all branches of banks.
4. Due to time constraint the researcher couldn't properly explore the proof of concepts in adequate testing environment and data.
5. Determine the impact level of trust, ethical conduct, and culture on the process of CSRM development and implementation in banking sector.
6. To make users life easy , this research work shall be changed to research project based on model that was proposed by this research framework and better to create some mechanical or robotic techniques to implement quantitative measurement of judgments(to avoid some subjective decisions of High, Low, or Medium)

References

[1] Abiy, W., and Lemma, L. Information Security Culture in the Banking Sector. Ethiopia. 5th ICT 2012 Ethiopia Conference. Venue: UN ECA, Addis Ababa, Ethiopia, (2012),

[2] Ana-maria, M. nizol & F. Gheorghe, "Audit for information system security", Informatical economical Vol, 14, no. 1/2010, pp5, 2010, retrieval from http: // revistaie.ase.ro/content/53/049620 suduc, % 2013, 201, %20Filip.pdf, last accessed on October 2012.

[3] Anene, L. N., & Annette, L. S.. An Architectural and Process Model Approach to Information Security Management. Lawrence Technological University. (2007)

[4] Anon International Journal of Electronic Security and Digital Forensics [Online] 2(3), P.306–321Retrievedfrom: 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, (2009).

[5]. Bel G.Raggad & Emilio Collar," The Simple Information Security Audit Process: SISAP",IJCSNS International Journal of Computer Science and Network Security, Vol-6,No 6 ,June 2006,retrieved from http://papaer.ijcsns.org/07-book/200606/200606c10.pdf Last accessed on January 23,2013.

[6] Catherine, D. "Introduction to Research Methods a Practical guide for any one undertaking a Research Project", Oxford, 2009, 4th Ed.

[7] Ettaul1, L. Rathod, V. "The zachman framework, the owner's perspective & security" retrieved from http://www.mcs.csueastabl.e.Last accessed on March 2013.

[8] Franklin D. Kramer, An Integrated Governmental Strategy for Progress, IOSR – JCE pp. 136-150, (2011),http://www.jstor.org/stable/43133822.

[9] Fredrik. J. B. Discovering information Security Management. Stockholm: Department of Computer and Systems Sciences Stockholm University & Royal Institute of Technology. (2005).

[10] George, S., Dawn, C., Andrew, M., Randall, T., Timothy, J. S., & Lori, F. Common Sense Guide to Mitigating Insider Threats 4th Edition. Software Engineering Institutes. (2012).

[11] Griffin L. K. "Analysis & comparison of DODAF and ZACHMAN framework for use as the Architecture for the united states coast guard's Maritime patrol coastal (WPC)",

2005retrievedfrom http://www.nps.edu/faculity/01sen/student.thesise/stetanou.pdf,last accessed on December 06, 2012

[12] Halefom, THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA, 2015

[13] Heru et al., Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05 (2011)

[14] Hessetbech J. and Herrman, C. "Globalized solutions for sustainability in manufacturing". Proceedings of the 18th CIRP international Conference, 2011. Retrieved from http://books.google.com.et/books?id=ZE9BXSVOTwC&pg=last accessed on Jan, 2013.

[15] Institute for Development and Research in Banking Technology (IDRBT). IT Governance Series: Information Security Governance for the Indian Banking Sector, Version 1.0, an IDRBT Publication. , 2011

[16] 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.

[17] ISO 27002:2005 "Information technology security techniques code of practice for information security management", 2005, retrieved from http://www.iso27001security.cost/html/27002.html,last accessed on March 20, 2012.

[18] ITU. "Understanding Cybercrime" *A Guide for Developing Country*. Geneva: International Telecommunication Union (ITU).2009

[19]. Jimmy, 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.

[20] Marshall B. Romaney & Paul John Setinbart, "accounting Information system" person prentice Hall 2009 Ed 11

[21] Michael, L. Information security architecture Building security into organization. 2007

[22] Mohammed, A., & Karen, N. Proceedings of the 7th Australian Information Security Management Conference: A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. 2009.

[23] Muniru,U,Zuraini.bt Ismail and Zailani.M, "A framework for the governance of information security in Banking system", IBIMA publishing Journal of information assurance & cyber security, 2011 retrieved from

http: //www.ibimapulishing.com/journals/JIACs/2011/726/96/726/96. Pdf, last accessed on January 23, 2013.

[24] NIST. Framework for improving critical infrastructure cyber security, version 1.On-line available:http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-_nal.pdf, February 12, 2014.

[25] Olayemi, O. J. "A socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria", International Journal of Sociology and Anthropology, vol.3, pp. 116-125. (2014)

[26] Onwubiko, C. "A security audit framework for security management in the enterprise", Global Security, Safety, and Sustainability: 5th International Conference, ICGS3 2009, London, UK, 1–2 September, 2009

[27] Official site of Zachman International Enterprise Architecture, www.zachman.com

[28] Pany, K. "Praud in a financial statement Audit", December 2002, retrieved from http: // www.aicpa.org/interst areas /forensic and valuation /resource/fraud privation Detection response / downloadable documents/student/20froud/20manual,pdf,last accessed on march 2012.

[29] Patrick, D. G. Managing Information Security Risk: Organization, Mission, and Information System View: U.S. Special Publication 800-39(2011).

[30] Peter Heraof, "Open-source security testing methodology manual", 2001, retrieved from http: // www.ideah/amster.org.last accessed on October 10, 2012.

[31] Puja S. Mandol and M. Verma, "formulation of IT Auditing standards", Seminar Organized by National Audit office, on China, September 2004, retrieved from www.endo.gov.en/uploadfile/newfile/20066/2113459150.doc,last accessed on October 11, 2012.

[32] Reserve Bank of India, "Information System audit policy for the Banking and financial sector" working group for information systems security for the banking and financial sector, department of information technology, reserve bank of India, Mumbai, October, 2001, retrieved from, http://rbjdoes.rbi.org.in/rdocs/publishtionreport/pdfs/26986.pdf,last accessed on March 2013.

[33] Rittenberg. L. E. Schwieger, B. J. Johnstone, K. "Auditing a business Risk approach be as 2008, Thomas corporation.

[34] Robert M. Slade, "security Frameworks" retrieved from http: // victoria.to.ca/techrev/rms.htm,last accessed on November 01, 2012.

[35] Santos, H. & Periora, T. " A security framework for Audit and management Information system security" IEEE/WIC/ACM International conference on web Intelligence and intelligent agent the chorology, 2010, retrieved from http: // www.researchgate.net/publishing/224187157

[36] Seribd, "Networks security Audit", February 2010 retrieved from, http: //www.scribd.com/doc/12734608/security-Network-Audit-Steps, last accessed on November 2012

[37] Tan, M.T.K. and Hall, W. Beyond Theoretical and Methodological Pluralism in Interpretive IS Research: The Example of Symbolic Interactions Ethnography, Communications of the Association of Information Systems, 19(1), (2008).

[38]. Tarimo, C. N. "ICT Security Readiness Checklist for Developing Countries, Stockholm; Department of computer and Systems Science, Stockholm university, 2006

[39] Terry. T and Robert K., "Intrusion Detection and Information Security Audit, IGI Global, 2007, retrieved from http: // www.hiltbrand.net/docs/auditing.pdf,Last accessed on December 01, 2012.

[40] Venkatesh, V., Brown, S. A., & Bala, H. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems.MIS quarterly, 37(1), 21-54. (2013)

[41] Wikipedia free encyclopedia, http: // www.en.wekipedia.org/wiki/wikipedia:free encyclopedia.

[42] Yigezzu.B, "Information System Security Audit readiness in case of Ethiopian government organizations. 2011, retrieved from http: // www.spidercenter.org/sites/defult/files/master-thesessponsoret/Ms-thesis-jorro.pdf.lastaccesses on July 2012.

Appendix's

ST.MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

FACULTY OF INFORMATICS

Dear respondent,

First of all, I would like to thank you in advance for devoting your precious time to fill in the questionnaire. This questionnaire is prepared to assess the Ethiopian Banking Industry's Cyber Security Auditing experience and readiness for implementation of cyber security audit and exploit as an input for developing a new cyber security audit framework. The information that you provide will be used to undertake a study entitled "**Cyber Security Auditing Framework For Banking Sector In Ethiopia"**

The study is done as part of partial fulfillment of Master of Science in Computer Science. The information you provide will be very confidential, and hence, I kindly request you to carefully and attentively read all the questions and give your genuine answers to the best of your knowledge. Your data is expected to contribute for the success of the study tremendously. If you have any enquires, you may contact me via the address stated below.

Tesfaye Asfaw Getahun

E-mail: tesfish680@gmail.com

Mobile: +251-911-167235

Thank you so much for your cooperation in advance.

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. PROFILE OF RESPONDENTS

1. Sex:

   Male ☐ Female ☐

2. Age:

   20-30 ☐ 30-40 ☐ above 40 ☐

3. Marital status:

   Single ☐ Married ☐

4. Educational Level:

   Certificate ☐ Diploma ☐

   First Degree ☐ Masters and above ☐

5. Your Profession:

   Computer Science ☐ Computer Engineering ☐

   Information System ☐ Business Field ☐ Others ☐

6. Position:

   Security Officer / Expert ☐ Risk Analyst ☐ IT Auditor ☐

   Database Administrator ☐ System Administrator ☐

   Controller Fiancé Auditor ☐ Other ☐

7. Department you work for:

   IT/ MIS ☐ Risk ☐ Control ☐ Other ☐

8. Work Experience:

   0-3 years ☐ 3-5 years ☐ 5-10 years ☐ above 10 years ☐

Part II. Cyber Security Policy and Standards

1. Do you have Cyber Security policy document to ensure the security of your Bank's cyber system? Yes ☐ No ☐
2. If your answer is no, what is the reason and your future plan with this regard?

   _____

   _____

   _____
3. If your answer to question # 2 is yes, to what extent it is ……?

   Implemented ☐ In plan for implementation ☐

   Not implemented ☐ Not in plan for implementation ☐
4. If your answer is "yes "for Q1.How often do you update the Cyber Security policy document?

   Annually ☐ Every two year ☐

   Never updated ☐ Others ☐
5. What standards or framework you follow in the process of implementing of your Cyber Security System?

   ISO/IEC 27002:2005:2. ☐ Industry Standards ☐

   COBIT ☐ .PCI-DSS ☐

Others, please specify_____

6. If you have cyber 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 ☐
7. Does your bank have a dedicated individual (or individuals) with responsibility for cyber security?

   Yes ☐ No ☐
8. How do you rate the management support in cyber security auditing process?

   Low ☐ Medium ☐ High ☐
9. Does the bank have annual budget for staff Cyber Security awareness program and technical training for its relevant staff?

   Yes ☐ No ☐

10 Do you think that separating Cyber security team from other IT staffs structurally under IT department is advantageous from Cyber security auditing perspective?

Yes ☐ No. ☐

If the answer is No, why?

_____

_____

_____

11. Do you think that lack of experienced staff on international standards, lack of local cyber security Framework/standard, and budget are problems that hindered the implementation of cyber security System in your bank?

Yes ☐ No ☐

12. Does the bank have formal risk management mechanisms?

Yes ☐ No ☐

13. 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 ☐

Part III. Physical and Environmental Security

1. How do you rate the physical and logical security facility implemented to protect Cyber Security System of your organization?

   Excellent ☐ Very good ☐

   Good ☐ Poor ☐

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. 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 ☐

5. Do you have security control for the third parties or for personnel working in secure area?

Yes ☐ No ☐

Part IV. Organizational Security

1. Is there management body that ensures the management support for Cyber system security in your organization?

Yes ☐ . No ☐

2. Is there management authorization process in place for any new information processing facility including all new facilities such as hardware and software?

Yes ☐ .No ☐

3. How do you rate the management's support to implement security?

Excellent ☐ Very Good ☐

Good ☐ Poor ☐

4. Is there defined inventory or registry maintained for the important assets associated with each cyber security system?

Yes ☐ No ☐

5. Do you have defined information classification scheme or guideline in place, which will assist in determining how information is to be handled and protected?

Yes ☐ No ☐

Part V. Personnel Security

1. Does employees' written job description include responsibility for information security?

Yes ☐ No ☐

2. 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 ☐
3. Are employees sign confidentiality or non- disclosure agreement as a part of their initial terms and conditions of the employment or on internal memo?
   Yes ☐ .No ☐
4. Do you have verification checks on permanent staff at the time of job applications?
   Yes ☐ No ☐
5. Do you have written incident Management and formal reporting procedure to handle security incidents?
   Yes ☐ No ☐
6. How often your organizations give IT use and security awareness training to staff, venders and/or customer?
   Don't conduct awareness ☐ .Once a year ☐
   . Twice a year ☐
7. How do you rate technical staffs' awareness about emerging technologies and related control issues?
   Excellent ☐ Very good ☐
   Good ☐ .Poor ☐
8. Does the bank have disaster recovery plan?
   Yes ☐ No ☐
9. Does the bank perform periodical penetration testing of their infrastructure?
   Yes ☐ No ☐
10. Does the bank have an approved business Continuity plan?
    Yes ☐ .No ☐

Part VI. Communication and Operations management

1. Do you have any operating procedures such as back-up, equipment maintenance, etc.?
   Yes ☐ .No ☐
2. Is antivirus installed and regularly updated on the computers that exist in your organization? Yes ☐ No ☐

3. Is all the traffic originating from un-trusted network into the organization checked for viruses?

   Yes ☐ .No ☐

4. Is back-up of essential information taken regularly?

   Yes ☐ .No ☐

5. Does management review internal control reports and initiate corrective action where necessary?

   Yes ☐ No ☐

Part VII. Access Control

1. Is there defined access control policy document?

   Yes ☐ No ☐

2. Is there any formal user registration and de-registration procedure for granting access to multi-user cyber security systems and services?

   Yes ☐ .No ☐

3. Is allocation and use of any privileges in multi-user cyber security system environment restricted and controlled?

   Yes ☐ No ☐

4. Do users sign a statement to keep password to the organizations critical infrastructure or resources confidential?

   Yes ☐ .No ☐

5. Do you have a process to review user access rights at regular intervals?

   Yes ☐ No ☐

6. When a new system (such as Firewalls, Routers, Switches etc) is installed on the network. Does any unnecessary protocol and services will disable /close the network?

   Yes ☐ .No ☐

Part VIII. System Development and Maintenance

1. How do you rate a culture of conducting cyber security requirement study before systems development in your organization?

Excellent ☐ Very good ☐

Good ☐ Poor ☐

2. Are security requirements derived from a business risk assessment?
   Yes ☐ No ☐

3. Is there a culture of conducting cyber security requirement study before systems development and test its security related issue in your bank?
   Yes ☐ No ☐

Part VIIII. Compliance

1. 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 ☐

2. Do you have audited your cyber security in a regular base?
   Yes ☐ No ☐

3. Have you outsourcing the cyber Security audit to third party?
   Yes ☐ No ☐

4. Are risks from third party access identified and appropriate security controls implemented?
   Yes ☐ No ☐