ADDIS ABABA UNIVERSITY COLLEGE OF NATURAL AND COMPUTITIONAL SCIENCE SCHOOL OF INFORMATION SCIENCE

DESIGNING A MULTI-TIERED SECURITY ARCHITECTURE TOWARDS INFORMATION INFRASTRUCTURE PROTECTION FOR NBE.

By
Chamo Gezahegn

October 2020
Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY COLLEGE OF NATURAL AND COMPUTITIONAL SCIENCE SCHOOL OF INFORMATION SCIENCE

DESIGNING A MULTI-TIERED SECURITY ARCHITECTURE TOWARDS INFORMATION INFRASTRUCTURE PROTECTION FOR NBE.

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

By
Chamo Gezahegn

October 2020

Addis Ababa, Ethiopia

ADDIS ABABA UNIERSITY
SCHOOL OF
INFORMATION SCIENCE

DESIGNING A MULTI-TIERED SECURITY ARCHITECTURE TOWARDS INFORMATION INFRASTRUCTURE PROTECTION FOR NBE.

By

Chamo Gezahegn

September 2020

Name and signature of Members of the Examining Board

Workshet Lamenew (Ph.D.)	_____	_____
Advisor	**Signature**	**Date**
_____	_____	_____
Examiner	**Signature**	**Date**
_____	_____	_____
Examiner	**Signature**	**Date**

Declaration

I, Chamo Gezahegn, hereby declare that the work which is being presented in this thesis entitled "Designing A Multi-Tiered Security Architecture Towards Information Infrastructure Protection For NBE." is an original work of my own and prepared under the guidance of my supervisor Dr. Workshet Lamenew. It has not been presented for any scholastic achievement in any University. All the sources of the materials used in this research have been duly acknowledged.

Signature: _____

Chamo Gezahegn

This thesis has been submitted for examination with my approval as university advisor.

Advisor's Signature: _____

Workshet Lamenew (Ph.D.)

Dedications

This thesis is dedicated to my parents, national bank of Ethiopia IT staffs and my colleagues who sacrifices all they have, their unconditional love and inspiration to make my dreams real.

Acknowledgment

First and foremost, I would like to thank Almighty God, who kindly help me to complete my thesis. without his blessings, this achievement would not have been possible.

I would like to give special appreciation and thanks to my advisor Dr. Workshet Lamenew for his continuous support of my research, unceased guidance, motivation, enthusiasm and immense knowledge. He has always been there providing his heartfelt support and guidance at all times.

A special thanks to National Bank of Ethiopia staff, specially Information Systems Management Directorates management and employee, who have spent their precious time and responded to all my interview, survey questions and later evaluating the architecture. Thank you for spending the time and sharing your views, perceptions, feedbacks and experiences with me in such detail.

Finally, thank you my family and friends for your support in every aspect of my life.

Abstract

Banking industry have increased dependency upon technology solution that enables their financial products and services but the convergence of technology renders to increasingly vulnerable to malicious attacks. As such, the need to ensure information infrastructure protection of the banking industry is a must and hence designing security architecture ought to be seen as a good manner.

Multi-tiered security architecture is a term which has different security technologies and measures to protect against different vectors of attacks. The main objective of the thesis is to investigate and design a multi-tiered security architecture towards information infrastructure protection. To achieve the main objective, it's imperative to identify factors affecting information infrastructure protection. Therefore, a security architecture consisting three main themes: communication network, associated software's and delivered services was used to identify current practice in information infrastructure protection of the bank.

Design science research methodology was employed to approach the design and development of the architecture following Peffer et al. (2007) process model. The design and development of the architecture passed through several stages, initially factors affecting information infrastructure protection were identified using the quantitative, qualitative, observation and network traffic analysis tool, and then these were used as design inputs. There were multiple brainstorming sessions for the design enhancement as participative modeling was the overall approach for the architecture design. Given the difference in scope and magnitude of the challenges identified in the study, the proposed architecture approaches information infrastructure protection through continuous improvement.

The architecture was finally evaluated in terms of component's completeness, comprehensiveness and fitness to the organization through an evaluation questionnaire and expert interview, accordingly, the developed architecture has capable to protect information infrastructure of the organization.

Key words: security architecture, information security, multi-layer security, multi-tiered security architecture; information infrastructure protection.

Table of Contents

Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

II	**Information Infrastructure**
IIP	**Information Infrastructure Protection**
NBE	**National Bank of Ethiopia**
COBIT	**Control Objectives for Information and Related Technologies**
ISP	**Internet Service Provider**
VPN	**Virtual Private Networks**
DMZ	**Dematerialized Zone**
IPS	**Intrusion Prevention Systems**
IDS	**Intrusion Detection System**
WAF	**Web Application Firewall**
DBF	**Database Firewall**
IT	**Information Technology**
ICT	**Information and Communication Technology**
CIA	**Confidentiality, Integrity and Availability**
IS	**Information Security**
ISS	**Information System Security**
ISA	**Information Security Architecture**
INSA	**Information Network Security Agency**
OSSIM	**Open Source Security Information Management**

Chapter one

Introduction

1.1 Background

Banking industry have increased dependency upon technology solution that enables their financial products and services but the key challenges that facing banking industry is how to adopt new technology with in organization in a timely manner (Chris P.,2013).

The highly growing interconnectivity of information technology systems and its convergence of technology renders to increasingly vulnerable to malicious attacks (Ramadan and Hefnawi, 2007). The Ethiopian banking industry is one of the most growing sectors of the country and It is now taking the industry by storm both public and private, banks are scrambling to make use of the latest banking technologies (Abiy W. and Lemma, 2012). Banking industries are seeking to use information technology for processing information in order to provide service for their customer and they are highly dependent on their information systems to carry out their activities. Because of this strong dependence on information technology, the number of attacks for the system is increased from time to time and any attempt which leads to compromise of availability, integrity, confidentiality (CIA) through unauthorized access and loss of information will affect the business at all.

The confidentiality, integrity, and availability (CIA) are well-known models for security policy development, used to identify problem areas and necessary solutions for information security (Terry C.,2013).The application of information and polices, communication technologies, techniques and strategy of the implementation for services of banks which has very important and all bank concerns and it is a prerequisite for local and global competitiveness(Akinlolu A, 2007). Information evolution has enabled different organizations which bring an opportunity to come across and communicate each other throughout the world (Johnson et al., 2015).

The development of information technology brings many advantages however beside advantage they introduce the challenge for protecting information infrastructure for an organization (Parsons et al., 2010). Information security has become major concerns and challenges facing organizations (Dutta A. and McCrohan R., 2002).

In today's technological and social environment, security is a very important part of a banking and financial institution system. With highly dependence on automated transactions, it is very

important to have a good security practices which are reliable for organizations, business and as individual to secure information. Business partners, suppliers, and vendors require high information security from one to another, particularly when providing mutual network and information access (Siponen et al., (2007). Survey conducted by Ethiopian cyber security emergency and readiness team stated that Ethiopia is facing huge amount of cyber-attacks which targeted different institution with different interest, and many attacks happened on different institutions country wide (INSA,2020).

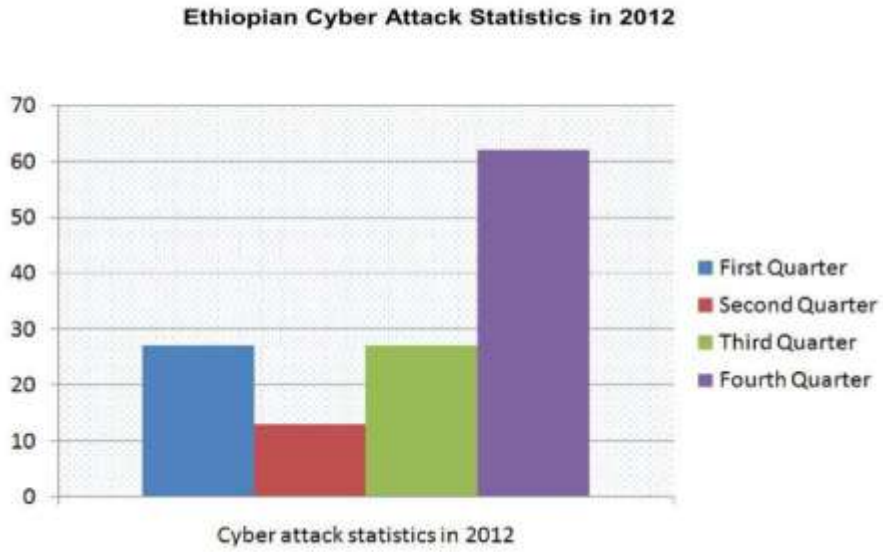


Figure 1.1 cyber-attack statistics (INSA,2020)

To mitigate cyber-attack identifying the current challenges of organization is the first hand and based on the gap identification the protection method is proposed.

1.2 Motivation

National bank of Ethiopia is a connection with all private and governmental banks, microfinances and many transactions are pass through NBE whereas INSA stated that there is a growth of cyber-attack which compromises resource of the Ethiopian financial institutions (INSA,2020). Security is complex and the weakest link of security is human beings (Schneier, 2000). To secure the NBE assets and resources all stockholders must aware and respond to their responsibility. The motivation behind this study is desire to learn the difficulties or challenges on

the area of information security architecture for NBE, theoretical and practical knowledge on the domain to identify gaps so that based on gap security architecture is design.

1.3 Statement of the Problem

There is a growth of cyber-attack on developing country due to wide spread of information evolution and internet connection (Johnson et .al, 2015). The advancement of information technology has brought many benefits, but the protection for information security and infrastructure is one of the main challenges of different organizations.

There are many studies which were conducted on the area of information security architecture by different scholars to help one of the core principle of information security: confidentiality, integrity, and availability. Bell-Lapadula has developed confidentiality model, Biba and Clark-wilson have developed integrity models and Chinese wall and Graham Denning has developed availability models (Nash and Brewer, 1989; Clark and Wilson, 1987; Bell, 2005 and Biba,1977). Also, different organizations and author have proposed different approach in designing information security architecture (BS 7799-2, 2002; Trcek, 2003; Anderson, 2003; Rees, Bandyopadhyay & Spafford, 2003; META Group, 2003 and Tudor, 2000). BS 7799-2(2002) proposed information security management based on the continuous cycle of activities by so-called PDCA (Plan Do Check Act) and it is cyclic model which ensures the best practice of organizations. The scope of ISMS is defined and the information security is established during the plan phase. The main focus of this study on the establishment and implementation of information security policy and it is repetitive approach which emphasized the fact that the security program cannot be complete 100% but it does not attempt to give procedure on the synchronization and inter-dependency of controls to be implemented. Trcek (2003), proposed the layered multi-plan model for information systems security which attempts to integrate existed approach regarding technological, organizational, and legal issues in the balanced way with the primary aim of protection and safeguarding of assets and to implement model, Trcek suggested system development and management approach which includes threat analysis, security infrastructure and public key infrastructure. This study recognized the importance of addressing the organizational aspect that cover the human resource management, organizational and legal issues. The problem of this architecture is that it does not address strategic issue, but it only depended on technical issues for system level. Rees et al. (2003), developed police framework for interpreting risk in E-Business security, and it offers a guide for implementing and maintain

security policy. They recognize the importance of developing and implementing the policy. The PFIRES model is based on the development of the product life cycle and software development life cycle, and it consists of four major phases: Assess, Plan, Deliver and Operate. This is to a certain extent similar to the Plan-Do-Check-Act phases of the ISMS proposed by BS 7799. However, the work of Ree et al. (2003), were mainly focused on the establishment and development of information security police which does not replace information security architecture but their lifecycle enables security architectures towards information security police and security awareness program. META Security Group (2003), recognizes the benefits of architecture-based approach towards information security architecture which reduces legal liability and improve security initiatives. They identify the information security architecture components and their information security architecture contexts are similar to PDCA model of ISMS and four phases of FFIRES model. They also proposed models which allows organizations to handle its current status of strategic level. Tudor (2000), developed information security architecture which includes risk awareness development process, assessment of current status and alignment of current and new controls to meet organizations need towards information security architecture requirements. He stated that security architecture is a process and it is not something that purchases. But this study cannot be comprehensive standard. J.H.P. Eloff, M.M. Eloff (2006), presents a state-of-the-art overview of distinguishable approaches, all attempting to define an information security architecture by a proposition of requirements for an integrated Information Security Architecture but there is no standardized, comprehensive information security architecture exists.

Stawowski (2009), Develop network security architecture by categorizing in to three layers like Perimeter section(router), Demilitarize zone (switch) and internal section (database and applications). He stated that When designing the security architecture recognized principles like compartmentalization, defense in depth, adequate protection should be taken into account to avoid the errors and achieve project cost-effectiveness. This study is the high-level architecture which cannot addressed standard security architecture by whichever one can agreed up on. Baharon, Shi, & Jones (2015), design Multilayered Security Infrastructure for IoT their objective was encrypted, decrypted and controlling access for both application and network layers. their study was limited on encrypting, decrypting and access control which cannot ensure the organizations systems security efficiently and effectively. Pauline K (2017), developed multi-

tiered information security architecture for information infrastructure protection for Kenyan banking industry. The study focuses on the technical part which includes the hardware, software and peoples who run the system. However, as the security is context dependent his study addressed the information infrastructure protection for Kenyan banks only. The security architecture that is appropriate for a bank cannot work for a hospital, university or military sector. Therefore, security architecture must respond to the context and culture of an enterprise (Peterson, 2006; Luker & Petersen, 2003). The study which were conducted on the area of information security architecture indicates that there is no standardized and holistic approach which address information security architecture for all organization and the available security architecture is highly context dependent. Consequently, it is reasonable to conduct security architecture study to a specific environment.

Therefore, as knowledge of the researcher this study design Multi-tiered security architecture towards information infrastructure that can be used to guide the NBE to ensure information infrastructure protection. This is achieved by: identify factors affecting information security architectures, based on the identified gap Design Multi-tiered security architectures and Finally, the developed architecture is validated.

To address the aforementioned research need, this research has set out the following research questions.

1. **What are the factors affecting the Information Security Architecture for IIP at NBE?**
2. **To what extent does Information Security Architecture suits NBE's IIP?**
3. **How valid is the proposed Information Security Architecture?**

The general objective of this study is to design multi-tiered security architecture towards Information Infrastructure Protection for the National Bank of Ethiopia.

Assess the current practice of information security architecture

Identify the major factors which affects information security architecture

Review related works on area of information security architectures

Design Multi-tiered security architectures

Evaluate the applicability of the designed security architecture.

1.5 Ethical Concerns

While conducting research there are various ethical concerns that need attention. The ethical issues might be related with the data gathering, disclosing research results and using other researcher material. In this research all the materials and sources, used as reference in this work was properly acknowledged, Privacy of the respondents was also properly contained; their responses were strictly confidential and only used for academic purposes and Conformance with the organizational policy and procedures with respect to any intellectual property rights of the organization.

1.6 The Scope and Limitation of the Study

The scope of this study was limited on National Bank of Ethiopia information infrastructure (Communication networks, Associated software's and Delivered services). This study employed design sciences research design and used quantitative, qualitative, observation and network traffic analysis tool for data collection. The researcher used survey questionnaire as a main tool and interview, observation and network traffic analysis tool as a support tool.

This research was limited on the technical approach of architectural design that can be implemented in the national bank of Ethiopia.

1.7 Significance of the Study

Given that attacks are getting more sophisticated with the advance in technology and connectivity, securing the information infrastructure cannot be overemphasized. This research endeavors to evaluate the gaps in the security architecture implemented to protect Information Infrastructure and develop a multi-tiered security architecture towards Information Infrastructure that can be more effective in protecting them. It is expected that as a benchmark study, the findings and developments are integrated into the subsequent protection of banking infrastructure.

For practitioners, this research help to secure information infrastructure for the National Bank that plays a crucial role in assisting information security officials to identify the vulnerabilities in their Information Infrastructure. It also outlines the current challenges in information security protection and the loopholes that exist in the implemented security architecture through which information security specialists and managers are able to identify the Information Infrastructure and evaluate whether their Information Infrastructure is protected with the aim of improving information infrastructure protection.

For researchers, this study is useful since not many studies of this nature have been undertaken in Ethiopian banking industry and it serves as a starting point for the researcher who want to conduct more comprehensive research in this area from the Ethiopian banking industry perspective.

1.8 Organization of the Thesis

The study has six chapters and organized as follow.

Chapter One: This chapter sets out a foundation for the thesis. It begins by providing a background for the study and discusses the statement of the problem, the aim of the research and the research questions to be addressed. It also presents the significance of the research and defines the scope and limitation of the study.

Chapter Two: This chapters described a general understanding of main concepts such as security, architecture, information security architecture, challenges of information security architecture, information security management, application of security architecture, development of multi-tiered security architecture for information infrastructure, enterprise information security architecture framework. The final discussed related works to present the distinction between this study and previous works.

Chapter Three: This chapter presented research design and methodology which includes general insight on the existing research methods and discussed the research method that was employed in this thesis.

Chapter four: Deals with the data analysis and design search process as per the data collected through questionnaire and interview, and the findings from the analysis were discussed in each section providing inputs to the design process.

Chapter five: Deals with the artifact design and evaluation, where the proposed architecture was designed and developed based on in depth discussion of the main findings in the fourth chapter, the demonstration and evaluation of the Proposed architecture.

Chapter six: The final chapter provides discussion, conclusion, recommendations of the study and future study suggested.

1.9 Operational Definitions

Attack – This is an event on a system whose main aim is to destroy, steal or alter information on a system.

Information infrastructure (II) – This is the communication network, associated software and delivered services that are used in an organization to enable communication or interaction between business or organizations and people.

Information infrastructure Protection (IIP) – This is the method of ensuring that the communication network, associated software and delivered services that are used in an organization to enable communication or interaction between business or organizations and people are not vulnerable to attacks.

Security - The quality or state of being secure that is to be free from danger.

Availability- Ensuring reliable and timely access to and use of information

Asset-anything that has value to the bank.

Confidentiality - Ensuring that access to information is appropriately authorized.

Design Science -Design science research methodology produces a new artifact that provides a technology-based solution to a relevant problem with significant impact and research contribution.

Information security- Is the preservation of Availability, Confidentiality and Integrity of information.

Integrity- The preserving the completeness and accuracy of the information which are processing by different methods.

Information asset- All documents, data, records and systems created managed, owned by the bank.

Information security incident- It is a serious of information security events which are unexpected and unwanted that have a great probability to compromise information security.

Information privacy- The capacity of a group or individual to protect or stop information about themselves from those which are not allowed to access.

Risk- The probability that threats that cause vulnerabilities on asset or loss to the asset.

Vulnerability – This is any weakness in a system that makes it possible for a threat to cause it harm.

Threats – This is any event that tries to exploit any vulnerabilities.

Security architecture- It is a model of how to make logical sense of relationships among several factors that have been identified as salient to the problem.

Multi-layered security architecture – A setup that uses different security technologies and measures to protect against different vectors of attacks.

Chapter two

Literature review

2.1 Overview

The goal of this chapter is to review relevant literatures in the domain area of information security architecture with a particular focus on information security architecture towards information infrastructure so as to provide a context for the study and clarifies the relationship between this study and previous work in the field. With this goal, in this chapter, a review of different literatures that are related to security architecture with implication to multi-tiered security architecture are discussed. This chapter is organized in to six main categories to have a logical flow of ideas and concepts in intention to put the whole research in perspective. The first category strives to bring a general understanding on basic concepts such as Security, Architecture. Then the second category of the literature review is presented information security architecture and factors which are important to have good information security like Information Security evolution, Goals, Policy, Standards & Checklist and Management. Then the third category of the literature review is presented to give insight on current gaps of information security for Ethiopian banking industry. Fourth, come up with Multi-Tiered Security Architecture, Information infrastructure protection, security architecture benefits. Fifth category describes how to design and develop multi-tiered security architecture with its components and network security. Finally, discusses about Enterprise Information Security Architectures Framework and a review of related works was conducted so as to present the distinction between this work and previous works.

2.2. Literature Review and Search Strategies

2.2.1 The Research Systematic Literature Review Process

Systematic literature review brings a benefit for a research to have good understanding about what he/she is study in a broader set of study which include all relevant studies and It also provides general view that enable researchers to understand all previous and current study area of the interest to confirm, reject, contrast or complement the previous study(Aline D et al, 2015).

It is important for a researcher to aware all about the previous study of the area and identify gap analysis. Gough et al. (2012) stated that the research must be understanding and investigating problems in a systematically. It is very difficult to address all studies on the area without the systematic literature search strategy.

Systematic literature review is secondary study which is used to identify, collaborate, evaluate, consolidate and map the output of the relevant primary studies (Tranfield et al. ,2003; Kitchenham ,2010; Seuring and Gold ,2012). This systematic literature review shows that the reviewer is unbiased, accurate, replicable, auditable and updated (EPPI Centre, 2013; Gough et al., 2012; Kitchenham, 2010). So, the new research that cannot consider the results of the previous work may results irrelevant, unethical or unnecessary works (Gough et al., 2012; Seuring and Gold, 2012). For this study all relevant research study was included to the best of the knowledge of the researcher and are analyzed.

2.2.2 Search Strategy

Search strategy is the best way to guide researchers to manage all important information of the researched area. The search strategy answers the question of what to search? (the area of the study), Where to search? (search engines and databases) How to minimize bias? (it should address the minimization of bias and the extent of the search based on resource availability) Which study is considered? (inclusion and exclusion criteria) What are the extent of the search be? (By considering all the available resources on the area) (Brunton and Thomas 2012; Hammerstrom et al., 2010). The literature review of this study was conducted following Bieser and Hilty (2018) search guidelines. The researcher started by identifying the main search terms based on the research questions: security architecture, information security, information security architecture, multi-tiered security architecture; information security architecture analysis, information security architecture model, information security architecture design; multi-tiered security architecture towards information infrastructure protection. For all of the main search terms, an alternative search terms were derived by finding synonyms (e.g., "multi-tiered" or "multi-layered").

An overview of the search terms used in the literature search is provided in Table 2.1 below.

Main Term Security	Alternative Term
architecture	Information security architecture, IT security architecture, information system security architecture
Information	Information substructure,
infrastructure Protection	infrastructure Defense, guard
Multi-tiered Security architecture	Multi-layered Security architecture

Table 2. 1Main and alternative search terms for the structured literature search

The sequence of activities to select eligible literature are started from screening, the process of identifying the relevant study (Brunton et al., 2012). The screening process needs identification of each study which was found (Adler and Van Doren ,1972) and the aim of this is not understanding of the subject but it is a quick reading whether it is helping to answer the research question or not. For screening phase, the title and abstract are used to select the literature and study which are not related are excluded with their described reason. Many studies are excluded because of duplication (Brunton and Thomas, 2012). The second process is reading phase, which needs analytical reading which is detail understanding of the study. Finally, the selected publications are added that are related to the area. Brunton and Thomas described the process of selecting relevant literatures which described in the following:

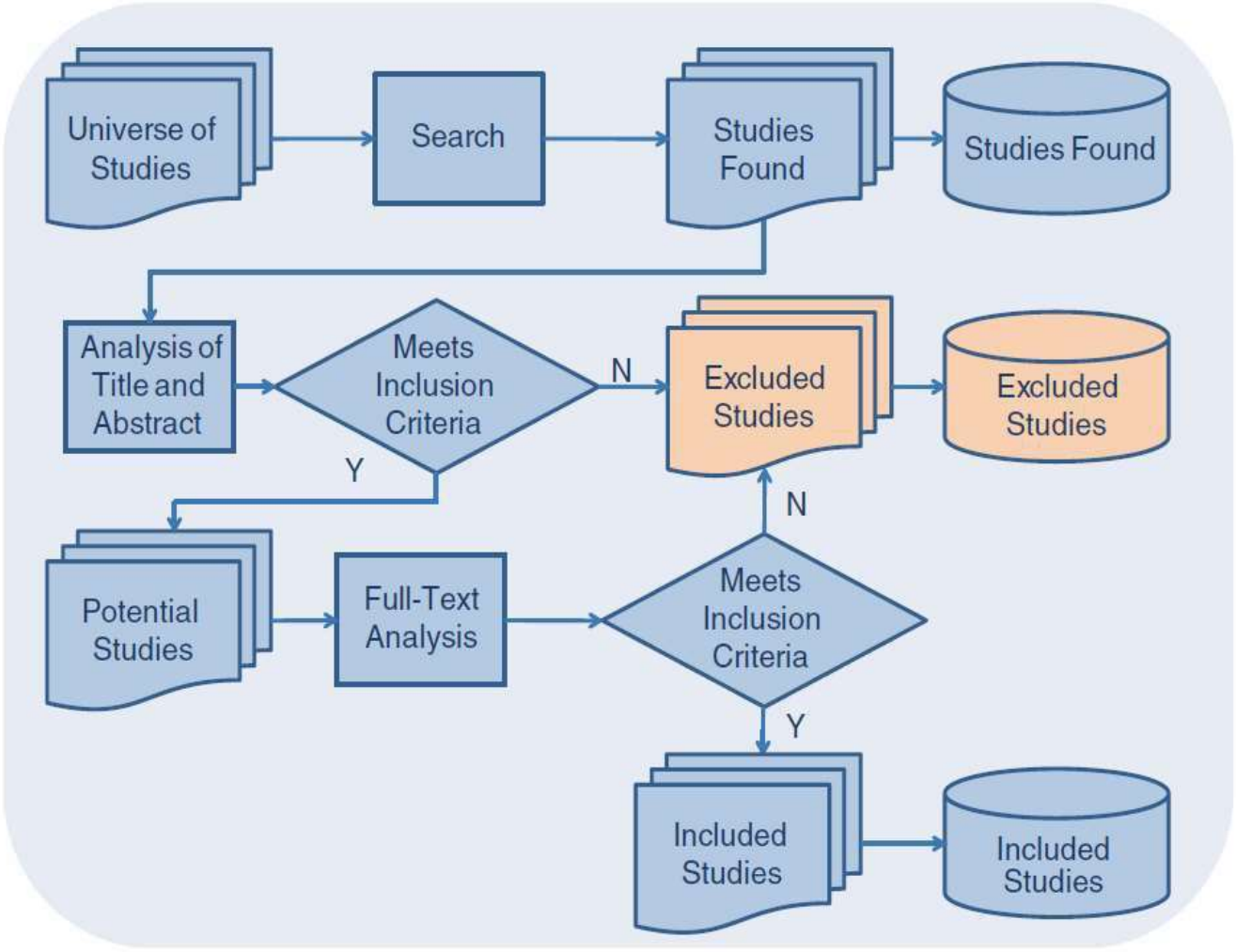
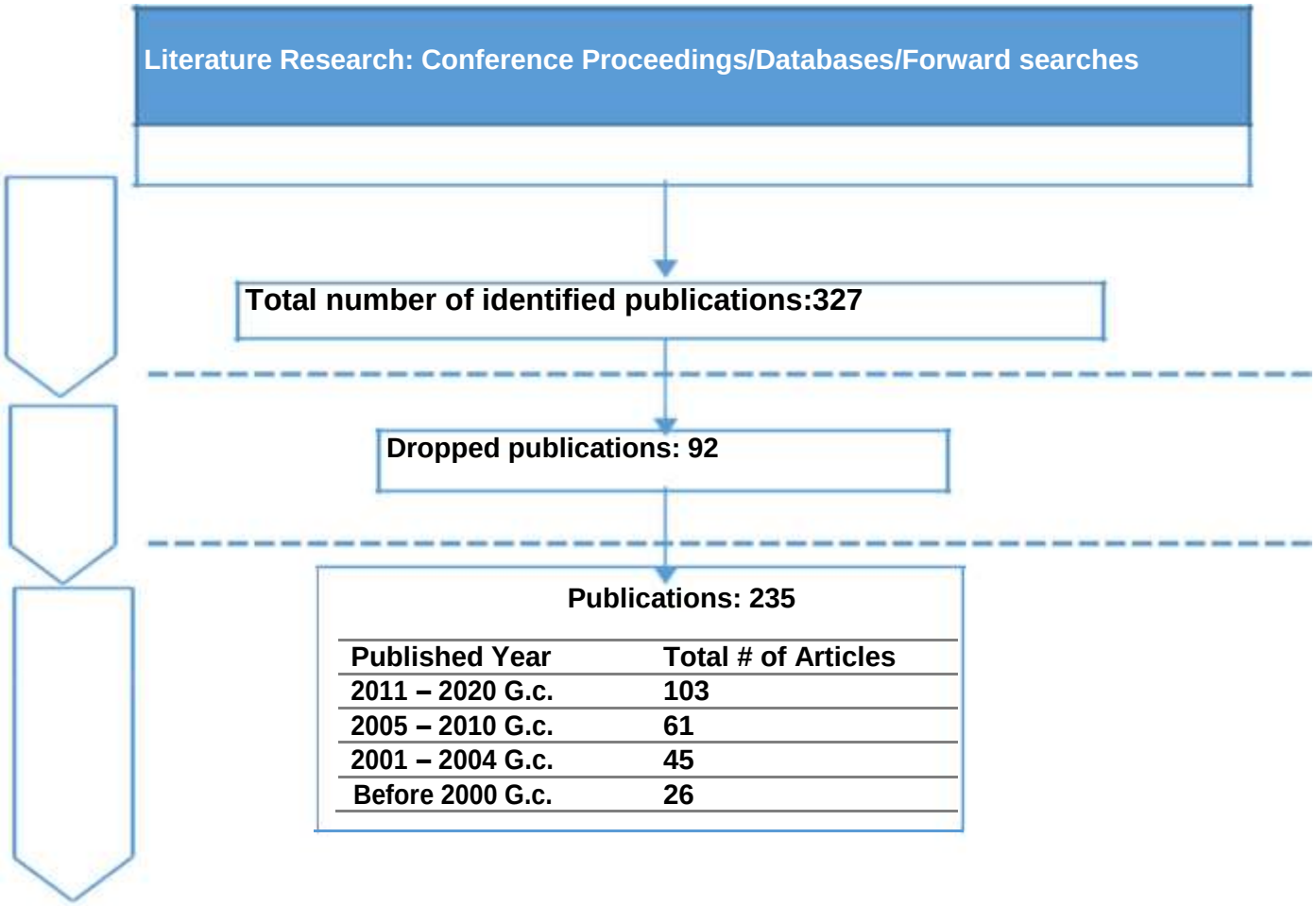


figure 2.1 Search process, eligibility and coding (Brunton and Thomas,2012)

The most used databases and platforms used by researcher were Sematic Scholar, ScienceDirect, ACM, AIS, IEEEXplore, Google Scholar, and Google.



Published Year	Total # of Articles
2011 – 2020 G.c.	103
2005 – 2010 G.c.	61
2001 – 2004 G.c.	45
Before 2000 G.c.	26

Figure 2.2 Number of search queries, volumes, identified and dropped publications.

2.3 Security and Architecture

2.3.1 Security

Until the end of 1980 security was limited to military only and it reveals the ability of military in war and reveals peace after war but now in the information age information security has become the main concern of an organization. In the information age security is not as simple as past because the whole world (government, public, private, military and educational institutions) connected each other through digital communications and it plays important role in creating competitive advantage (Killmeyer, 2006). The security is among the top concerns of the organization (Kappelman et al., 2013)

What is Security? According to Webster, Security includes measures taken to guard against espionage or sabotage, crime, attack, or escape. It is the way of minimizing the risk of any assets which include a person, community or organization and all resources to vulnerabilities (Anderson, 2003). A term Security used in the sense of minimizing the vulnerabilities of assets and resources (Bayle, 1988). The word security tied with control and risk since control are implemented to control risks to reduce losses that may be caused by attackers (Kim & Leem,2005; Porter et al.,1985). Security is the quality of being secure and to be free from any danger or building protection from adversary that cause danger from those who would do harm, intentionally or otherwise (Singh et al. ,2014). It is a Measures taken to protect a system, or the condition of a system that results from the establishment and maintenance of measures to protect the system. Alternatively, defined as the condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss (ITU-T, 1991; SHIREY ,2000). The security of information and its systems entails securing all components and protecting them from potential misuse by unauthorized users (Balcha, 2005). The ultimate purpose of security is to never permit the enemy to acquire unexpected advantage (USAF, 2003).

There are Three fundamental qualities of information which must be taken in place to protects information from threats which includes confidentiality, integrity and availability.

In order to adequately protect its operations and assets successful organization should have the following multiple layers of security in place for the protection of its operations (Dwight A,2013; Singh et. al,2014; Solms & Niekerk ,2013).

Computer security: is the way of securing computer information and goal of computer security is the confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information resources.

Physical Security: secure physical objects, items, other area of company from misuse or access of unauthorized user.

Personal Security: to secure group of individuals who are allowed and authorized to access operations and organizations.

Operations Security: to safeguard details operations or activities of organization. Communications Security: to secure communication technology, media and content of the organization.

Network Security: to secure connections, contents and network components. Information Security: to safeguard and protect critical elements of information including hardware and software.

2.3.2 Architecture

The term architecture has been used for many years with in the field of information technology to refers and provide a guidance to software systems and application developer. Oxford dictionary define the term architecture as the conceptual structure and logical organization of a computer or computer-based system. Architecture must be Layered and is a metaphor derived from building trade like the homeowner designing a home, information technology professionals provide architectural drawing for enterprises information system and processes. It is a high-level drawing that does not change with tactical decisions to improve technology and it is like a framework of business processes and information that they need (Harmon P.,2002; DeLooze LL,2001; Heaney J et al.,2002, Harjinder S.,2010).

There are different types of architecture under the area of information system such as: network architecture(provides a mechanism for more easily understanding the communication flows between the various systems that exist within the network.), system architecture(the hardware components and communication channels that connects to form networked systems), software architecture(computational components like information, flow control, styles, object based and layers), information architecture(the information centric-view of the systems) and security architecture(styles in which organizations information are protected and safeguarded). (Edward A., 1999; David Garlan & Mary Shaw,1993; Harjinder S. ,2010; D. Comer, 2005).

2.4 Information Security

Information security is an effective implementation of policies to protect information and assets from theft, tampering and manipulation to ensure confidentiality, integrity and availability with the well-informed sense of assurance that information risks and controls are in balance (Stephen S.,2005; James M.,2005; Munk ,2015; H. G. Goldman,2010). Information security is the protection of information and its critical elements which include information security management, computer security management, data security management, data security and network security by using hardware to collect, store and transmit such information. (Balch, 2005; Dwight A,2013).

Generally, Information Security is related to government laws and regulations, international standards that prescribe practices perceived as necessary which make organizations deploy, define or establish roles and responsibilities, strategies, processes, organizational structures, policies, technologies and other measures (Antonio Eduardo & Ernani Marques,2015; Albuquerque Junior & Santos, 2014).

There are many inhibitors of information security which include: Lack of security awareness, lack of training for staff ,Lack of allocated funds due to low priority ,No negative experiences so it is assumed that everything is ok, Resistance to set up a uniform user interface across the organization, Lack of consistency of risk management processes across the breadth of organization, Expectation of users to be able to access all information when they want, Security perceived as hindering productivity(SIFT,2007; Stephen Smith ,2005). Information security are three measure which includes: Administrative measures (change people's behavior which affects the organization and its members), Technical measures (affect the technology which are used to process information, store information, ensure access information by legitimate users only), Physical measures (to protect information and assets by physical mechanisms) (Bjorck, 2005).

2.4.1 The Evolution of Information Security

The knowledge of information security was beginning during the second world war when millitorrs used mainframe to store information and ensures the confidentiality and integrity of the data. The evolution of the information security model has occurred due to the evolution of the type of threats that businesses were faced on a day-to-day basis. Because of sophisticated technology which was launched from time to time the challenges of information security was very bold. When internet was launched every customer, company, contractor, consultancies were sharing information across and between different stakeholders. Now we are on the age of 3G,4G and 5G by which threats have evolved and become more and more sophisticated. Mostly known information security threats are: threats happened during technology implementation phase like viruses, worms, distributed denial of service and the mitigation methods are firewalls, anti-virus, and IPS. Human related threats were like device miss-configurations, excessive trust in security technology, and security flaws within the technology itself. (Mark R., 2013; Michael E& Herbert J., 2012; Mahi & Anup N., 2009).

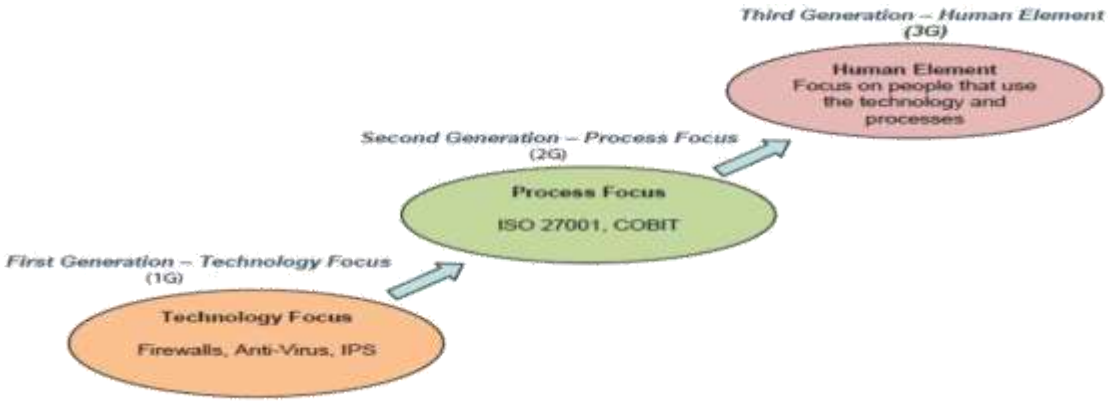


Figure 2.3 **Evolution of Information Security (Mahi & Anup N., 2009)**

2.4.2 Information Security Goals

The goal of Information security is ensuring the confidentiality, integrity, availability, accountability and assurance so that any kind of sensitive information cannot be accessed, disclosed, modified, disrupted and destructed by unauthorized body (Mcumber,1991; Solms, 998; Mark R., 2013; Singh et al. ,2014; Pfleeger, 2003; Gollman,2006; Johansson & Johnson, 2005; Kim & Leem, 2004; Bruner ,2001; Damien H. and Matthew W;2003; Mark S & Jim B,2014; ITU ,2008).

Confidentiality

Confidentiality means that the information that should be secret and only those authorized to access it may receive access (Michael E.,2012). It is ability to carry out an external task which restricts information flow (Zwick and Dholakia ,2004). It is of making sure that information is only seen by people who have the right to see it (Singh et al., 2014). Avery key component of protecting information confidentiality would be encryption by ensures that only the right people can read the information. The common confidentiality threats are malware, intruders, social engineering, insecure network etc.

Integrity

Integrity is concerned with the trustworthiness, origin, completeness and correctness of information as well as the prevention of unauthorized modification of information (Michael E.,2012). It is the Mechanism to ensuring that information remains intact and unaltered. It includes both the correctness and the trustworthiness of the data. There are two broad mechanisms for integrity, the preventive and the detective. Preventive mechanisms are like

access controls which prevents unauthorized modification of information and detective mechanisms are intended to detect when preventive mechanisms failed in case of unauthorized modification (Singh et al., 2014).

Availability

Availability is the means of the accessing information by owner when it needs to access. In simple words it is the uptime of computer-based services (Mark R., 2013; Singh et al., 2014). The common availability threat prevention methods are regularly doing off-site backups and redundancy can limit the damage caused by damage to hard drives or natural disasters.

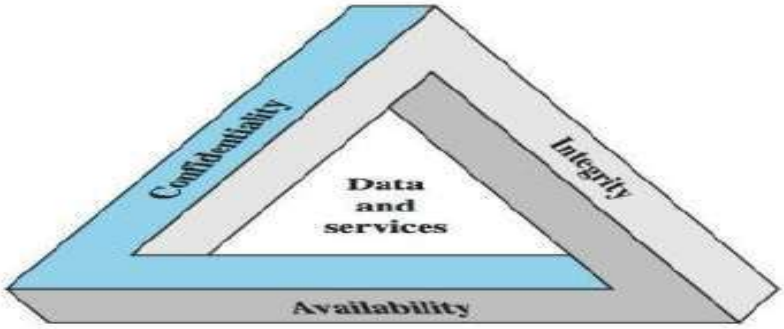


Figure 2.4 The CIA triad (Singh et al., 2014)

2.4.3 Information Security Policy

The absence of the standard information police are the major challenges of many organization to secure their environments (Kark et al., 2007). Information security policy is the set of rules, standards, practices, and procedures that the company employs to maintain a secure IT system and credibility of the entire information security program of an organization depends upon a well-drafted information security policy (Knapp, K,2009; Peggy E.et al. ,2013).

Many researchers identify that the information security policy development is one of the practical ways of protecting information system of an organization and It is also the first step towards preparing organizations against internal or external attacks (Kadam, A,2007; Myyry,2009).

The characteristics of a secure system is a system which have a good and specified security policy(Jim Alves-Foss et al., 2004).There are four common security bases which includes police (high-level statements which guides developers, installer, maintainer and user), standards (the way to configure, install and use), procedure (step by step instruction according to police and standards)

and guidelines (recommendation about security) (Mark R.,2013).Common Information Security Policies are Access Management Policy, Acceptable Usage Policy, Network Security Policy, Data/Information Handling Policy, Internet Usage Policy …etc.(ISO/IEC 27001,2009; Harold F., Micki K ,2007 ; SANS ,2002).The objective of information security policy is to ensure information protection, business continuity, company reputation, enforcing law, responsibility and accountability for Information Security in the organization (Mark R.,2013; Michael E.,2012; SANS ,2002).

2.4.4 Check Lists, Standards & Best Practices of Information Security

Information security has their own checklist, standards and best practices which were practiced in numerous organizations in an exceedingly different context. Check list are an honest thanks to moves from unskilled approach to structured way that ensures security in a very certain level. BS7799-1 and Basic Protection Manual (BSI, 2002) are the foremost well-known checklists (Zuccato, 2002).

Security standards are a listing of artifacts and techniques that address all aspects of security like Confidentiality, Integrity and Availability which secure different area of enterprise (Yang et al.,2010). The well-known security standards are like ISMS, concentrate on managing information security ; BS7799 (ISO27001), concentrate on managing information security; COBIT, help managers to manage the danger related to IT and planning, management and implementation of IT. ; Information Security Forum (ISF), were used as a general guideline and good practice for information security; Generally accepted system security principles (GASSP), were it are used as a general guideline and good practice for information security; baseline protection Manual (BSI IT), were it is used as a general guideline.

Information security best practice comprises different sub-standards and various areas like Guidelines for Management of data Technology Security (GMIT), help managers to manage the chance related to IT and planning; management and implementation of IT (Ekstedt and Sommestad, 2009). Whether or not Check lists, standards & best practices are many advantages they need also disadvantage is that every best practice just covers one dimension of enterprise security like network and physical security.

2.4.5 Information Security Management

Information security management is the way of ensuring organizations business continuity and preventing information security incidents that affects organization in any way. Information security management is systematic ways of organizing people, information technology systems and processes that keeps critical systems from internal and external threats (Cardno, C. A., 2019). The object of the information security management is to convert organizational security policy in to a set of requirements that can be communicated to organization in any ways (Tracey, R.P,2007). Information security management must be in a holistic way which requires a well-established information security management system which address all aspects of organization that create and maintain secure information environment (Jan Eloff And Mariki Eloff,2003). ITU (2008), stated list of Secure management components include; Policy management, Secure access management, Encryption of network management traffic, Secure remote access for operators, Firewalls, Intrusion detection, Application security layer and Virus free software.

2.5 Current gaps in Information Security Challenges for Ethiopian banking industry.

The main challenge of many organizations are not only how they secure their information infrastructure, but also how they require new platforms and intelligence to secure their infrastructure which might be improperly disclosed, modified in an inappropriate way, destroyed and lost which can result in financial losses and damages to reputation (Wichita R &Ugander R,2014; Blakley et al., 2001;Peggy E. et al,2013).The followings are the major identified challenges of information security which were addressed by different literatures which needs great attention to handle.

2.5.1 Human factors in Information Security

The weakest link of information security is human being. Organizations are highly dependent on the users which are great achievement on the inside threats because security policies are enforced by people to ensure organizations information protection (Schneier, 2000). Many experts of information security believe that a good behavior of user make effective information security in an organization (Stanton et al.,2005). There are two factors of human behaviors: the technical and intentional expertise. The technical expertise is mainly targeted on skill and knowledge of the user while intentionality expertise focused on the action of user whether beneficial or harmful. The knowledge and skills acquired can be a good approach for enshrining security architecture towards information infrastructure protection.

2.5.2 Vulnerabilities and Threats that cause risk on information security

Vulnerability is a weakness in information security procedure, asset, design and control that can be intentionally or accidentally with goal of causing security breach (Whitman and Mattord, 2003; Mark R.Jason L.,2012). It is a weakness in a system's design, implementation, operation, management, software, hardware on a server and a client that can be exploited by a determined intruder to gain access to or shut down a network. (Joseph M,2009; ITU-T, 1991; SHIREY, R. ,2000). To this end, several organizations have been increasingly focusing on developing safety related policies and aligning them with non-organizational regulations (Cram et al., 2017).

Mark (2012) and Michael (2003) defined Information security threats as any event whether it is intentional or unintentional or either an action or an inaction to harm an organizations information system through destruction, denial of service, unauthorized access, modification and disclosure. It can come from myriad sources in our connected world and an organization must consider employees, contractors, and even the cleaning staff because any of these people could potentially be a threat, and cause damage (Warren P.,2008; ITU-T, 1991; SHIREY, R. ,2000; Sahare, Naik and Khandey ,2014). Motivations behind information security threats are ideology and the desire to challenge powerful interest, a desire to demonstrate technical proficiency, rebelling against the prevailing system of intellectual property financial benefit by displeased employees (Broadhurst et al.,2014; Edward W. et al. ,1997).

2.5.3 Information Security Culture

According to the report of UK governments 95% of incidents were happened due to cultural factors or behavior of people and only 5% is due to technological issues (Royds, 2009). Most organizations undergoing some form of traditional cultures which can impact attitudes towards security. Security culture cannot be assessed in isolation from the overall culture within a work environment this is because an organization's culture has a strong impact on organizational security (Ruighaver et al., 2007; A. Martinsi & Jan elop,2002; Thomas Schlienger &Stephanie Teufel,2003). A security culture is the way of performing security to everyone who have not allowed to access as a natural way of doing their job (Oost & Chew, 2007).

Organizational cultures are the understanding of the employee on polices and standards towards information security (McIlwraith, 2006). Therefore, to understand security culture it is first

important to have a grasp on the wider organizational culture. The followings are the factors which affect information security culture in a given organization such as Top management support, information security awareness, training, educations and accountability (Bulgurcu et al., 2010; Herath & Rao,2009; Kajava et al., 2007; Kim ,2014).

Top Management Support

Top management support refers decisions, investments and actions taken for enforcing information security policies across the organization. It refers to promote information security police and standards (Kajava et al., 2007; Lee et al., 2004). The priority concern of information communication technology is information security which is shared by top management to benefit an organization as whole and to initiate a culture of security awareness with in organization (Adnan R et al.,2017). The top management support can play crucial role for implementation of security policy and security governance in a given organization because the better the top management support information security the greater preventative efforts in a firm(Da Veiga, A& Eloff, J,2007; Kankanhalli, 2003; Tracey & R.P,2007; Von Solms,2006; Doughty,2003; Behling et al. ,2009; Omar et al. ,2016).

Information Security Awareness

Awareness is a process of changing the attitude of user on the security practice and its main purpose is to focus on security understanding which helps them to easily recognize and respond to security related issues accordingly (NIST ,2003; S.M. Furnell,2002). To improve the effectiveness of the security awareness, organizations need to introduce awareness program and social psychological principles (M.E. Thomson & R. von Solms,1998). As organizations are dependent on people, their awareness, ethics and behavior it must understand what they want to achieve if we are to accomplish the goals of the organization (Morrill, 2007).

Creation of security awareness include both individual and collective activities through email, pamphlets, formal presentation and discussion groups to increase user's knowledge and understanding of security policies and mechanisms in organizations (Hagen et al., 2013; Smith & Jamieson, 2006). Many studies noted that employee awareness is one of the best measures to protects a company's data (Hagen et al., 2008; Chang, A&Yeh, Q.,2006; M. Siponen,200; M.D. Krohn, J & L. Massey, 1980; Sang M. Lee et al., 2004).

Information Security Training

Training Provides skill in how the protection may be achieved. Kerry-Lynn et al. (2006), described that employees should learn, develop and integrate the proper information security skills into their daily behavior and, ultimately, facilitate the protection of knowledge assets. Training aims to know the amount of security which strives to supply security skills and skills which are acquired during training are built abreast of awareness. It seeks to show skills that allow a personal to hold out certain functions. Training on Security programs should decide to assure the protection policy legitimacy to safeguard the data infrastructure (Son, J,2011).

Information Security Education

Education integrates all security skills and collection of various security practices in to common body of data and therefore the main purpose of education is producing IT security specialists and professionals. Bensnard and Arief (2004) emphasize that education of staff is very important because it makes people awake to the consequences of their actions thus ensuring that individuals are tuned in to the threats and probable damages. It Provides deeper understanding of why protection is required (Steven Furnell and Nathan Clarke, 2005). Security education schemes should aim to form employees recognize the legitimacy of data security policy to safeguard the firm (Son, J,2011).

2.6 Information Security in Ethiopia Banking Industry.

The government of Ethiopia has realized information security as very important business accelerator by: Formulating legal framework to secure cyberspace, Develop and implement Cyber security affiliated national information and communication technology policy and strategy and finally, Develop and implement national spatial information and technology policy. Established Information Network Security Agency with council of Ministers Regulation No. 1340/2006 Prepare and enforce Critical Mass Cyber Security Requirement Standard (CMCSRS,2017).

Ethiopian banking industry offers credit facility, saving scheme, international banking and fund transfer (Simeneh, 2013). the major problems of these banks are information attacks both internally or externally. The banks are striving to achieve certain objectives like availability, integrity, confidentiality. the banking industry must balance between giving employees real-time access to applications and information, and addressing the corresponding concern for the security

of information assets and the information systems (Behabtu A.,2015). The two major identified security risks facing banking industry were data loss prevention and identity & access management (MWR,2010). The survey which was conducted by Halifom Hailu (2005), data collected from 40 institutions which are familiar with ICT and the respondents were from both government and private institutions. The Survey show that all respondents was experienced number of cyber-crime incidents. The result show that computer viruses, worms, malwares and other malicious attacks (57.1%), website defacement (40%), illegal access (17.1%), spam (14.7%) were the most perpetrated cyber-crimes against the institutions. The result also indicated that 62.9% are causes computer data damage,45.7% are causes denial of services and 45.7% are causes system interference.

2.6.1 Information Security for National Bank of Ethiopia

National Bank of Ethiopia is running a big project with INSA to develop Cyber Security Framework for Ethiopian Banking Industry with the initiative of NBE but this security framework is ongoing process and it is high-level. The bank does not follow any specific standard or best practice regarding security management and the Challenges of the bank include: Lack of experienced personnel, managements awareness on information security is very weak, Lack of industry standard or best practice locally (Abeselom N., 2015).

To overcome the above-mentioned problems of the bank developing multi-tiered security architecture can be the good approach. To develop architecture, it requires to identifies the current challenges and issues so that the gap can be identified. Finally, the security architecture is developed and it is incorporated under the enterprise security architecture.

2.6.2 Common Security Attacks on Banking Industry

The banking industries are experiencing lots of information security threats but the common one is Attacks Threatening Confidentiality, Attacks Threatening integrity and Attacks Threatening availability.

Attacks Threatening Confidentiality are categorized in to two styles like traffic analysis (refers other varieties of information collected by an intruder by monitoring online traffic) and data snooping (refers to unauthorized access to or interception of information).

Attacks which threating integrity are several types of attacks masquerading, modification, repudiation and replaying.

Attacks which threatening availability are mostly denial of service attacks (DOS) which slow, interrupt, busy or collapse systems by sending messages from every direction (Singh et al., 2014, Changsok Y. et al.,2015; Moore.T., et al.,2009; Gopalakrishna,2011).

As it is stated by (Changsok Y. et al.,2015) The most common interest behind attackers are seeking to acquire capital, confidential data and sensitive information. The most common attacks of the bank industries are the following.

TCP/IP SPOOFING- is the way by which illegal access is attempted on a system by sending an email message to a victim that appears to come from a trusted machine by spoofing machines' IP address. IP address spoofing is a powerful technique which enable hackers to send packets to a network without being blocked by a firewall. This is because usually firewalls filter packets based on sender's IP address and they would normally filter out any external IP address (ChangsokY. Et al.,2015).

Virus: A computer virus is a program that is configured to replicate itself across machines and corrupt computer files which including programs and as a result affect the operation of a system. These viruses can be gotten from normal web activities through opening files with virus infected attachments, installing of software, downloading and, accessing a site that has malware but to mention a few (Webroot, 2010).

Worms and trojan horse: Trojan horses and worms are the most frequently happened threats to the banks to lost the resources of information infrastructure. A worm is a program that replicate themselves on the computer network which perform malicious activities. Unlike worms Trojan horses are not replicate itself but they are destructive by riding computer of viruses to introduces viruses on your computer. (Madan Bhasin,2007)

Bot networks: programs that infect a system to provide control access and remote command via a variety of protocols machines for vulnerabilities and A botnet scans systems that can be exploited this includes antivirus software and firewalls (Rouse & Wright, Botnet, 2017).

Vishing: is a cyber-attack in which Voice over IP (VoIP) and social engineering are used to access the financial and private information from the public for getting financial reward. It is an illegal practice where an attacker calls a user and pretends to be from a bank in which the user has an account and asks to verify the user's account information and once the user gives his credentials such as username, password, credit card number, etc., the attacker has easy access to the user's account and the money in it (Moore.T. et al.,2009).

Denial of services: an attack in which a user or an organization is prevented from accessing a resource online (Rouse & Loshin, 2016).

Malwares: is a maliciously crafted software program that accesses and alters the computer system without the consent of the user or owner. Malware includes viruses, Trojan horses, worms, etc. (Gopalakrishna,2011).

PHARMING- attack whenever a user tries to access a website, he/ she will be redirected to a fake site. Pharming can be done in two possible by exploiting vulnerability in DNS server software and one is by changing host's files on a victim's computer (Moore.T., et al.,2009). CROSS-SITE SCRIPTING ATTACKS (XSS): are types pf injection by which scripts are injected from malicious as if like trusted source and so that it will be executed. these types of attacks are occurred when users are using web applications to send malicious codes using web browser for different users (Gopalakrishna,2011).

Phishing: is a kind of attack in which an attempt is made to obtain sensitive information of user such as passwords, credit card details, usernames etc. the most common tools include, Abuse of Domain Name Service (DNS), Botnets, Phishing Kits, Technical Deceit, Specialized Malware and Session Hijacking (Changsoky. et al.,2015).

2.7 Security Architecture Towards Information Infrastructure Protection.

2.7.1 Security Architecture

Security architecture is a term applicable to the wide verities of activities which are different in the level of details on which it acts. It provides a guidance for protection of information's in business, information system and technology levels.

Security structure as a unifying framework and reusable offerings that put into effect coverage, standards, and risk control selections. Open safety structure (OSA) defines the security architecture as the design of artifacts which describes IT architecture (Shahram J. & Farzaneh F.,2011; Peterson ,2006; Thorn et al, 2008 and Peterson ,2006; Tom Scholtz, et al., 2005). Security structure ought to also be a nicely-defined report which specifies protection services that provide how and where in an incredibly very layered model and its miles a cohesive protection design which address security requirements and become aware of what safety control are applied in (Prentice Kinser ,2007; Thorn et al., 2008). The information security architectures are accustomed guarantee protection domains which aligned company needs and business

method to work collectively otherwise commercial enterprise alignment and IT cause vulnerabilities of organizations (IBM, 2008).

2.7.2 Multi-layered Security Architecture

The Multi-layered security architecture is a setup which uses different security protection mechanism for different vectors of attacks. Every layer has its personal specific vulnerabilities, threats, attacks and mitigation strategies. (Krisztina C et al. ,2007; Pauline,2017). Multi-tiered security architectures as having or involving several awesome layers, strata, or degrees (Heiko Schuldt, 2008; Mohajerani MR, Moeini A,2002). The foremost common multi-tier structure together with a statistics control tier (database servers), a utility tier (commercial enterprise logic), a customer tier (interface capability) and net tier which exist between consumer and application layer (Heiko Schuldt,2008). ITU-T X.805, on the recommendation of protection architecture for a machine which deliver end-to cease communication ITU-T defined three protection layers which include: the infrastructure safety layer; services security layer; and also, the applications safety layer.

The aim of information security architecture is giving conceptual architecture design for information security by linking the components information security like security mechanisms, security infrastructure, security procedures and policies.

2.7.3 Benefits of Information Security Architecture

The first benefit of information security architecture is to Integrate different security elements like network, information and provide security services. The second benefit is to design a security by addresses the requirements like authentication, authorization and accounting by specifying what security controls are to be applied. The third benefit is to reduces the cost of security. The fourth benefit is to help change managements. The it divides the complex networks so that it can be easily managed components and these separated components are used for planning and identifying security threats and run security solutions for logically existing networks. The final benefit of information security architectures is for compliance (Tahajod et al, 2009; Prentice Kinser ,2007; Office of CIO,2010; Farah,2004; Peterson ,2006; SABSA,2008; Preez and Pieterse ,2009). The overall aim of Security architecture is generalized as holistic approach, security & business alignment, Integration, change management, security requirements analysis, security cost reduction, and compliance.

2.7.3 Information Infrastructure Protection

The concept of information infrastructure is that the combination of knowledge and infrastructure technology which may be a shared, open, heterogenous and evolving technical systems and it includes the data technology, operations and peoples (Hanseth ,2002). Atkins et al defines information infrastructure as "...hardware, software, personnel, services and organizations" (Atkins et al., 2003, p.13). The most tools to attack systems are malware (virus, worm, Trojan horse) to switch and destroy information (Eugene NICKOLOV ,2005). Information infrastructure is that the technological and human components, networks, systems, and processes that contribute to the functioning of knowledge system (Braa et al.,2007). It is the communication network, associated software and data resources that are employed in a corporation to enable communication or interaction between business or organizations and folks (Paulin,2017). The measure of knowledge infrastructure protection must be implemented to mitigate the attacks. There are three strategic objectives to prevents information infrastructure attacks: prevent cyber-attacks against information infrastructure, reduce national vulnerabilities to cyber-attacks, minimize the damage and recovery time from cyber-attacks. (Eugene Nickolov ,2005).

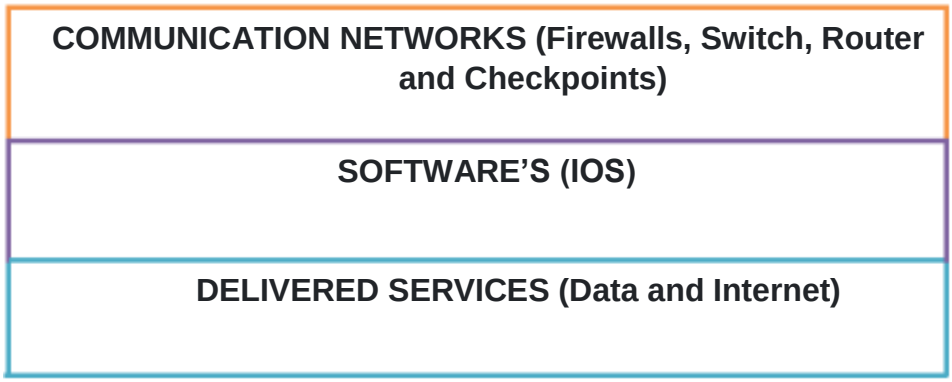


Figure 2.5 Information infrastructure components (Pauline,2017)

2.8 Design and Development of Multi-Tiered Security Architecture for Information Infrastructure.

Security architecture design and development is a key factor which helps security engineers to grasp necessary security mitigations strategies and understand flow of information between the components. (Sarah Pramanik & Northrop Grumman ,2013). To develop multi-tiered security architecture there should be regulation or guideline on the bottom within the organization and these guidelines are taken as a framework. Lack of the way to implement information security

for information infrastructure protection for IT professionals are the most important problems of the many organizations (Benson Young,2012). The multi-tiered security architecture must be designed in the way of benefitting organization which should be integrating various components, managing risks, supported the most effective practices and financially feasible (Thorn et al., 2008). On this study the researcher adopted the Farah method of design information security architecture which have Three steps.

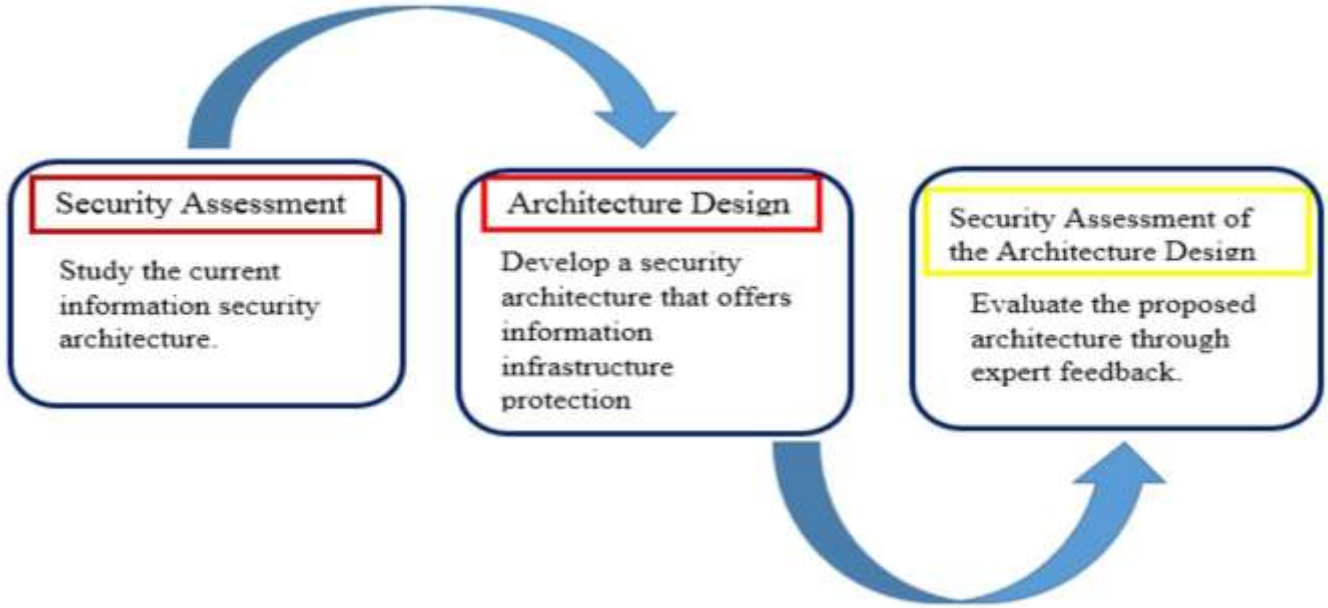


Figure 2.6 Steps Adapted in Designing a Security Architecture from Farah (2005)

1. Conducting security assessments: this step is important to identify current security architecture and its main aim is to evaluate the threats and vulnerabilities of organizations system.

2. Formulation of target security architecture designs: are based on the finding of the first phase security architecture will be developed.

3. Evaluate the efficiency and effectiveness of the developed architecture by expert feedback.

2.8.1 Multi-Tired Security Architecture Components

The information security architecture must be holistic to perform best and slot in to the businesses seamlessly and integrate technology, people and processes. Awareness of specific components of multi-tiered security architecture enables security personnel, users and regulatory aspects to have a good knowledge of security architecture. The components of multi-tiered security architecture include: organizations infrastructure; Security policies, standards, and procedures; Security baselines or risk assessments; Security awareness and training programs;

Compliance; Monitoring and detection; Computer incident/emergency response and Disaster recovery/business continuity planning (Eloff & Eloff, 2005; Killmeyer, 2006).

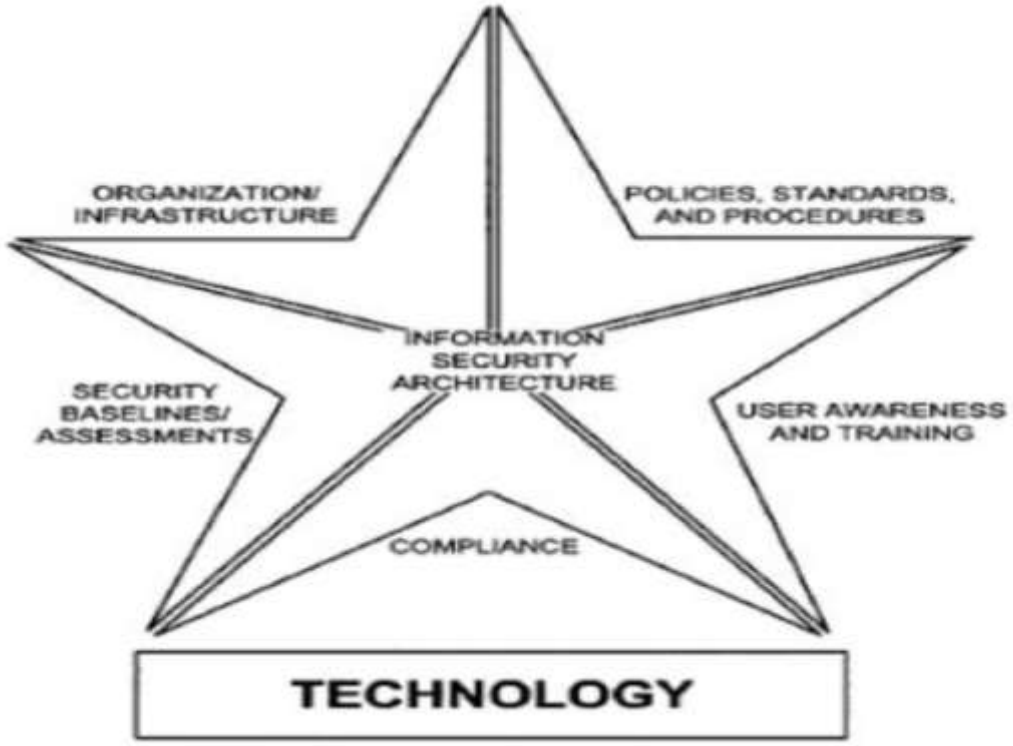


Figure 2.7 Information Security Architecture Components (Killmeyer, 2006)

2.8.2 Network Security

Network is one in all the most components of organization that has to be secure from any insider and out of doors attacks and it's crucial for IT systems and their good operation highly depends on its performance, reliability, and security. Fail of improving good network design costs company by losing business continuity, security incidents, cost of rebuilding network (Mariusz S. ,2009). The suitable design of the network security architecture provides many advantages just like the isolation of low-trust network area, Limitation of the safety breach scope, Accurate network access control, Quick identification of IT systems security incidents, Cost optimization and Ensuring basic attack vectors. (Mariusz S. ,2009; SecaaS,2012; Nilaykumar S. et al., 2013). Depending on the amount of the attacks and kinds of data that has been compromised the network attack causes several hours of downtime and it causes serious breach in confidentiality, integrity and availability of knowledge (Mohajerani MR & Moeini A., 2002). Securing network is vital as securing

computer and encrypting a message and that they identify the following that should be considered When developing network security (Mohammed m &Alexander a.2,017).

Access – authorized users are provided the means to speak to and from a specific network. Confidentiality – information within the network remains private to trusted staff or users. Authentication – make sure the users of the network are who they are saying they're. Integrity – make sure the message has not been modified in transit and is secured during transmission. Non - Repudiation – make sure the user doesn't refute that he/she used the network.

The security layers are categorized in to External or perimeter and internal layers. The perimeter security layer is formed from edge routers which offer first line of Dos protection and dedicated security device like firewall, check points, VPN, IPS, WAF. Internal security layer consists of firewalls, IPS (Mariusz S. ,2009). It also, includes security of physical environment and logical security components that are inherent within the services. The subsequent information infrastructure is going to be the primary group that has to be protected like Routers, firewalls, encoding using Virtual Private Networks (VPN), Intrusion Prevention and cargo balancing additionally because the core network services like core, distribution and access switches, server farm, server's application and databases must be protected too.

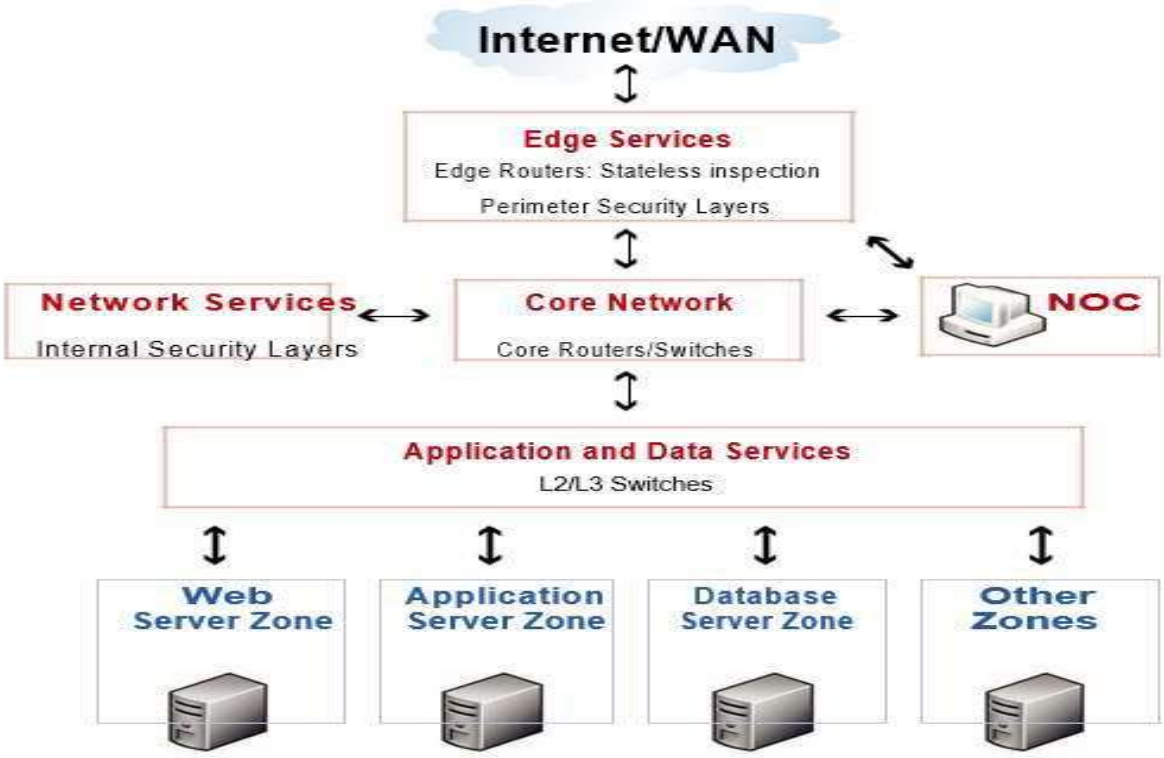


Figure 2.8 Network Security Architecture (Stawowski, 2009).

2.9 Enterprise Information Security Architectures Framework

The enterprise security principles are the main factors for planning, designing, implementing and operating of enterprise information security architecture by providing a good design decision and aligning to the business need requirements. due to continuous nature of data security architecture, lack of interoperability, lack business convergence, and lack business partnership the foremost focus of security architecture is on developing requirements, designing templets, developing models and incorporating principles (Gartner,2011; Keem & Leem, 2005; Jan Killmeyer,2006; Khayami,2010).

An enterprise uses security architecture for the following: it reduces the cost of organization on security, it helps for change management, it helps for an improved integration between security elements, security services and security mechanism and at the same time it allows the business and security staffs to align their efforts, it works as a holistic view that specifies which security services are provided, how and where and ensures compliance (SABSA, 2008).

Enterprise information security architectures are examined from abstraction to the general idea point of view. The abstraction level includes holistic methods versus partial methods (Nakamur, Hada, & Neyama, 2002; Rees, Subhajyoti, & Spafford, 2003; Shariati, Bahmani, & Shams, 2010). Holistic methods include the following: Gartner, Sherwood Applied Business Security Architecture (SABSA), AGM-Based SOAE Security Governance model, Intelligent Service-Oriented EISA and RISE (Shariati, Bahmani, & Shams, 2010). Sherwood Applied Business Security Architecture (SABSA) is one of a security-architectures which might be a risk-based methodology for delivering security infrastructure solutions that support new technological trends and opportunities (Sherwood, J., A. Clark, and D. Lynas ,2005). Gartner Enterprise information security architecture was introduced in 2006 by organizing EISA with EA program and collaborating them and it's focused on structure only but doesn't include methodology for implementing EISA (Oda et al.,2009). RISE Methodology is the excellent framework which was achieved by incorporating security and privacy features into business processes and emphasizes on the processes and lifecycles which should be implemented and uses standards (Anderson, J.A. and V. Rachamadugu,2008; Jianguang, S. and C. Yan., 2008; Korhonen, J.J., M. Yildiz, and J. Mykkanen. ,2009). AGM-Based SOAE Security Governance model is the merchandise of Appling ISO/IEC 17799 and SOGP to Agile Governance Model and it's accustomed suggest a

Governance Model for security requirements management within the context of service- oriented enterprise architecture (SOEA). (Anderson, J.A. and V. Rachamadugu,2008; Jianguang, S. and C. Yan., 2008; Korhonen, J.J., M. Yildiz, and J. Mykkanen. ,2009). Intelligent Service-Oriented EISA is model for the systematic and automatic management of EISA activities and risk management are supported ISO27002. (Anderson, J.A. and V. Rachamadugu,2008; Jianguang, S. and C. Yan., 2008; Korhonen, J.J., M. Yildiz, and J. Mykkanen. ,2009).

SABSA offers a framework and methodology in such the best way that it guarantees the protection of enterprise information through endless process. It is the developing information security architecture for a risk driven enterprise and its aim is to provide information security architecture for information infrastructure solution which helps business initiatives. The foremost features of SASBA is that every functionality relies on the business requirements analysis and it develops a sequence of strategy, design, implementation and lifecycle to stay up the business opportunities (Sherwood, Clark, & Lynas, 2009). Compared to the Gartner framework, which is extremely abstract and theoretical, SABSA is more acceptable because it's specific to the organization, highly customized to the unique model, their practice and holistic nature(Burkett, 2012; Shariati et al., 2011; John Sherwood, Clark, & Lynas, 2005; Coetzee& Marijke,2014; Alemu, Meskerem, and Abrehet Mohammed Omer,2014; Van den Bosch,2014). For this research SABSA is adopted because it is a strong and internationally recognized architecture methodology which focuses on the business requirements and develops from there and used over other methodologies because of its business focus and talent to trace controls back to those requirements.

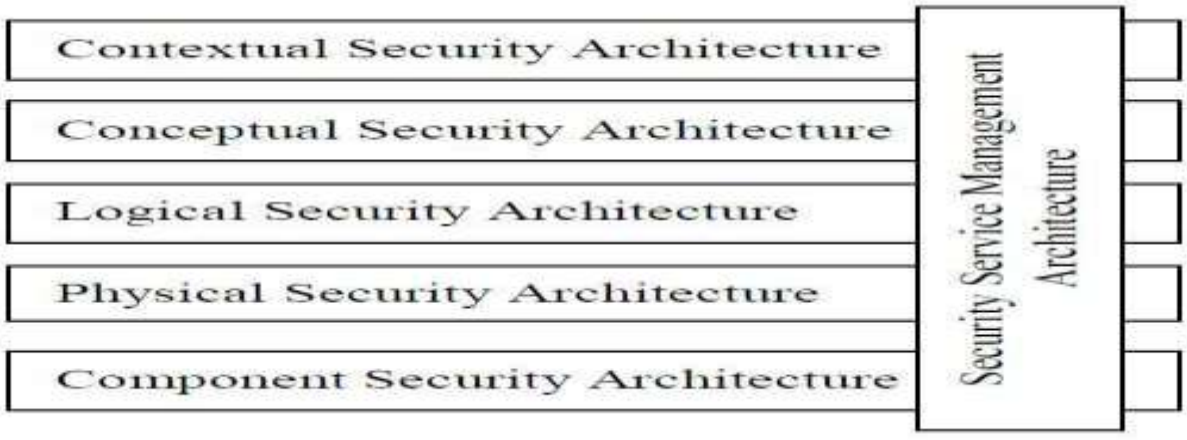


Figure 2.9.1 SABSA Model for Security Architecture (Sherwood, Clark, & Lynas, 2009)

	ASSETS (what)	MOTIVATION (why)	PROCESS (how)	PEOPLE (who)	LOCATION (where)	TIME (when)
Contextual Architecture	Business decisions	Business risk	Business processes	Business governance	Business geography	Business time dependence
	Goals and objectives	Opportunities and threats inventory	Inventory of operational processes	Organizational structure	Inventory of sites, places, etc.	Time dependencies of business objectives
Conceptual Architecture	Business knowledge and risk strategy	Business management objectives	Strategies for process assurance	Roles and responsibilities	Domain framework	Time management framework
	Business attributes profile	Enablement and control objectives, policy architecture	Process mapping framework	Owners, custodians, users, service providers and customers	Security domain concepts and framework	Through-life risk management framework
Logical Architecture	Information assets	Risk managenement policies	Process maps and services	Entity and trust framework	Domain maps	Calendar and timetable
	Inventory of information assets	Domain policies	Information flows, fuctional transformations	Entity schema, trust models, privilege profiles	Domain definitions, interactions	Start times, lifetimes and deadlines
Physical Architecture	Data assets	Risk management practices	Process mechanisms	Human interface	ICT infrastructure	Processing schedule
	Data dictionary and data inventory	Risk management rules and procedures	Applications, middleware, systems, security mechanisms	User interface to ICT systems, access control systems	Host platforms, layout and networks	Timing and sequencing of processes and sessions
Component Architecture	ICT components	Risk management tools and standards	Process tools and standards	Persomnnel man'ment tools and standards	Locator tools and standards	Step timing and sequencing tools
	ICT products including data repositories and processors	Risk analysis tools, risk registers, risk monitoring and reporting tools	Tools and protocols for process delivery	Identities, job descriptions, roles, functions, actions, access control lists	Nodes, addresses, and other locations	Time schedules, clocks, timers, interrupts
Service Management Architecture	Service delivery management	Operational risk management	Process delivery management	Personnel management	Management of environment	Time and performance management
	Assurance of operational continuity and excellence	Risk assessment, risk monitoring and reporting, risk treatment	Management and support of systems, applications and services	Account provisioning, user support management	Management of buildings, sites, platforms and networks	Management of calendar and timetable

Figure 2.9.1 The SABSA matrix from the business-driven approach. Adapted from (Sherwood et al ,2015).

The contextual security layer: it the development of the architecture from a business view and its goal is to secure goals, assets and objectives. The conceptual security layer: looks at the architectural view and its aim is to identify risks, risk management, process assurance, roles and responsibilities, domain and time management. The logical security layer: looks at the processes required to achieve security by identifying information assets, risk management policies, processes and services. The physical security layer: focuses on the data assets, risk management practices, human interface and ICT infrastructure. Component security layer: includes the ICT components, tools and standards for risk management, processes and personnel management. The security service management: aims to ensure that all layers are secure (Sherwood, Clark & Lynas, 2015). The following figures are the SABSA security architecture from the business-driven approach.

Related Works

There are works in this area that have been conducted with a particular attention to multi-tiered security architecture towards information infrastructure. Here presented are some notable studies. BS 7799-2(2002) proposed information security management based on the continuous cycle of activities by so-called PDCA (Plan Do Check Act) and it is cyclic model which ensures the best practice of organizations. The main focus of this study on the establishment and implementation of information security policy and it is repetitive approach which emphasized the fact that the security program cannot be complete 100% but it does not attempt to give procedure on the synchronization and inter-dependency of controls to be implemented.

Trcek(2003) proposed the layered multi-plan model for information systems security which attempt to integrate existed approach regarding technological, organizational and legal issues in the balanced way with the primary aim of protection and safeguarding of assets and to implement model but The problem of this architecture is that it does not address strategic issue but it only depended on technical issues for system level.

Rees et al. (2003), developed police framework for interpreting risk in E-Business security and it offers a guide for implementing and maintain security policy and he propose the PFIRES model that consists of four major phases: Assess, Plan, Deliver and Operate but this model does not replace information security architecture.

Pauline (2017) work on multi-tiered security architecture for information infrastructure the case of Kenyan commercial banks. The study was come up with the proposed architecture that were

significantly help to reduce the number of attacks for banking industry bases but the study was context dependent on Kenyan banks only.

Stawowski (2016) provided a security architecture that was done by underlining important for proper operation of IT systems as most applications work in the networking environment and It is well presented network security architecture which describe the important of security architecture for designing network that describes security zones and layers But because of Different IT systems have specific requirements that the network security architecture should fulfill this research was not standard security architecture.

Baharon, Shi, & Jones (2015) conducted the study on Multilayered Security Infrastructure for IoT and they addressed both application and network layers that were all encrypted, decrypted and access control mechanism but on their study limited on encrypting, decrypting and access control mechanism which cannot ensure the organizations systems security efficiently and effectively.

Eloff & Eloff (2016) develop security architecture by identified the components of information security architecture which includes security assessment, infrastructure, policies, user awareness, training and compliance but this architecture was context dependent.

Below are Summary of Gaps Identified from literature Review about Security Architectures.

Author and Year	Title	Objective	Methodology	Key Results	Identified Gaps
British Standard Committees (2002)	Information security management systems Specification with guidance to be used	Implementation of information security policy	Literature Review	Organizations are required to supply attention for information security police to assure organizations information.	The developed information security does not try to deliver tool on the synchronization and inter-dependency of controls to be finished.

Denis Trcek (2003)	An integral framework for information systems security management	Design the layered multi-plan model for information systems	Literature review	Build the layered model for information systems. joining various domain of IS security to Achieved optimal and Balanced solutions for an enterprise.	It does not deal with strategic issues but only tech nical problems on s ystem level version for data syst ems.
Jackie Rees, Subhajyoti Bandyopadhyay, And Eugene H. Spafford (2003)	Creating maintaining and effective security strategy and policy for software applications.	To developed framework for interpreting threat in E-commercial enterprise security.	DSRM	Build framework for interpreting risk in E-Business security.	The fact is that Information security policy does not replace information security architecture.
Pauline Kemunto (2017)	Multi-Tiered Security Architecture for Information Infrastructure Protection for Kenyan commercial banks.	To develop information security architecture for Kenyan commercial banks	Exploratory and Descriptive.	The developed security architecture for commercial banks of Kenya.	Develop architecture for the context of Kenyan selected commercial banks and the architecture is highly dependent on the polices, rule and regulations of the commercial bank of Kenyan.
J.H.P. Eloff& M.M. Eloff (2016)	Information Security architecture	The holistic approach for information security Architecture by describing the overview of all distinguishable approaches.	Literature Review	Describe the holistic approach for information security architecture in a distinguishable way. Identified the requirements for an integrated architectural approach to attain the max imum impact regarding or ganizational statistics prot ection.	Because of lack of standard security architecture this study was very low understanding about the knowledge of security architecture that is existed.

Baharon, Shi & Jones (2015)	A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing	Providing strong security schemes to protect mobile data.	experimental.	Develop Lightweight Homomorphic Encryption scheme which have Encryption and decryption methods to secure application layer and network layer of mobile IoT.	Security cannot be ensured only by encryption and decryption alone and these were not guaranteed to ensure efficiency.
Mariusz Stawowski (2016)	Network Security Architecture	To develop network security architecture	DSRM	Design of the network security architecture which provide isolation of low-trust systems, limitation of the security breach's scope, cost savings.	There is no standard security architecture so that ever one can agreed up on for this reason this study is the high-level architecture and cannot address all existing architecture.

Table 2.2 Summary of Gaps Identified from literature Review about Security Architectures.

Research Gap

Based on the literatures presented earlier, security architecture is the major concern. However, there are different kinds of security architecture which are varied from country to country and organization to organization. Moreover, the available security architecture is highly dependent on security guidelines, rule and regulation of an organization so it is highly context dependent. Therefore, this research addresses the multi-tiered security architecture towards information infrastructure for National Bank of Ethiopia, which is not addressed in earlier works.

Chapter Summary

The first section was intended to create a general understanding of main concepts such as security, architecture. The second section of this chapter presented the main parts of Information security such as evolution, goals, policy, standards, managements of Information security. The third section of this chapter discuss current gaps of information security in Ethiopian banking industry. The fourth section of this chapter discuss about the Multi-Tiered Security Architecture, security architecture, information infrastructure protection, benefits of security architecture. The fifth category describes how to design and development multi-tiered security architecture with its components. the final section discusses Enterprise information security architecture and related works.

Chapter three

Research design and methodology

3.1 Overview

The selection of research design and methodology must be based on the statement of the problem and research questions. The starting point of any scientific study is identifying the reason for conducting the research study. Research methodology is the systematic approach of understanding problems with the help to collect, analyze and interpret data. The ultimate goal of research methodology is supporting the research study to achieves its objective and it's also an umbrella of various research methods (Kothari, 2007). Selecting the appropriate research methodology is based on the nature of the research. This research aims to develop multi-tiered security architecture towards information infrastructure for application, network and databases by using existing literature review to identify current challenges of National Bank of Ethiopia. The nature of this research is characterized by types of application, network, databases and services existed in the National Bank of Ethiopia and how these information infrastructures are protected with the aim of developing multi-tiered security architecture.

3.2 Research Design and Methodology

Research Design

Research design provides a way to collect, analyze and interpret data. In this study the research follows design science research approach which is generally and widely used methodology within the area of scientific discipline. The studies that are focused on organizations employs design science to provide knowledge and it's relevant to bridge the gap between academic research and organization by addressing what's developed within the academy and what's applied within the organization (Romme ,2003).The design science paradigm is utilized because the standard research paradigms specialize in describing, exploring, explaining and predicting the phenomena and identify the link between them(Van Aken, 2004; Gibbons and Bunderson ,2005; Manson, 2006). Traditional research paradigms like natural and social sciences have limitation when the goal is design, construction and creation of recent artifacts and design science is suggested for conducting this type of research (van Aken, 2004; March and Smith ,1995; Le Moigne,1994; Romme, 2003; Simon,1996). Design science is a new research paradigm which operationalizes the research when the aim is artifacts or recommendations. Design science are

often performed in both academic and organizational environment (Aline D. et al, 2015). The goal of design science is to review, research and investigate the artifacts from academic and organizational point of views (Kuechler ,2011). It is also the rigorous process of designing the artifacts to resolve the matter, evaluate what was developed and communicate the result (Cagdas and Stubkjar, 2011). The output of this research is within the style of artifacts, general instantiation, abstract artifacts, constructs, models, frameworks, architectures, and style principles (Vaishnavi and Kuechler ,2015). Also, the goal of design science research isn't only to form an artifact but also to answer questions about them "are the artifacts useful?" (design an artifact that improve the problem) and "is the solution true?" (answering the knowledge question about artifacts are two styles of research problem which are studied deliberately science research methodology). (Johannesson and Perjons ,2014; Peffers et al.,2007).

This chapter describes the methodology which address the subsequent research questions:

1. **What are the factors affecting the Information Security Architecture for IIP at NBE?**
2. **To what extent does Information Security Architecture suits NBE's IIP?**
3. **How valid is that the proposed Information Security Architecture?**

These steps shall be adapted within the development of an architecture which can help to improve information infrastructure protection. The steps are as follows; Conduct a security assessment, formulate a security architecture design and Evaluate the effectiveness of the proposed architecture through expert feedback. This study developed a multi-tiered security architecture supported the subsequent process which includes: Identify the gaps within the current architecture, Development of security architecture and Evaluate the developed security architecture.

Research Methodology

There are different authors that formalized the research method for design science paradigm. Burge (1980), which developed the research methodology that differs from the traditional one by addressing the useful and applicability of technology. Takeda (1990), develop design cycle aimed to construct a model that support the development of the intelligent computer-aided design system. Eekeles and Roozmburg (1991), compare the traditional research method and propose a method for engineering related research through a design cycle. Walls et al. (1992), define and

design science research methods based on the products and process.Vaishnavi and Kuechler (2011), they improve the design cycle which was proposed by the Takeda.

An Aken (2004&2005), develop the research methodology for design science that reduce the gap between academic research and requirement of the organization to address solution for the organization problem. Then Cole et al. (2005), developed the methodology for design science which focuses on information system. Also, Manson (2006), developed design science methodology that proposed output of design science research based on the Vaishnavi and Kuechler. Peffers et al. (2007), consolidated the methods for conducting research under the design science research paradigm. Finally, Altruki et al. (2011), proposed method which derives from the synthesis of ideas formalized by several authors, particularly in the area of information systems which is referred to as the design science research cycle. There are many Design science process models presented in the literature as listed above and one of the common cited design science process is Peffers et al. (2007) which is useful for better understanding of process and steps followed in conducting research study and it is also used to understand and visualize steps to conduct study and process. It consolidates a method for conducting research on the area of design science paradigm. They were constructed design science process model with six steps which presented structure of principles and procedures used to develop a research. (Peffers et al., 2007).

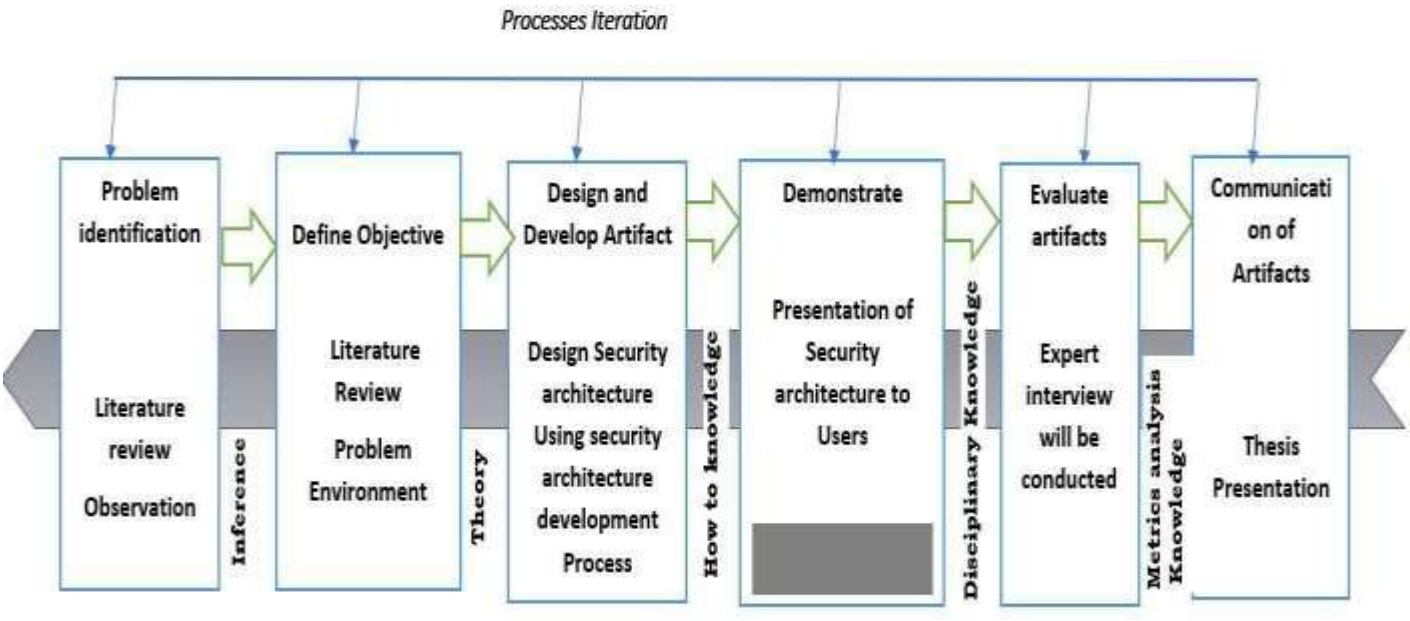


Figure 3.1 Design science research process (DSRP) model (K. Peffers, et al.,2007)

3.2.1 Problem Identification and Motivation

The first step in design science is to identify the problem and motivation for the study.

There was no study which conducted on multi-tiered security architecture on Ethiopian banking industry. The important of this study is that it is starting point for both academic and organizations about security architecture so that the detail will follow. Its relevance was protecting companies' information from cyber-attacks. The researcher was understanding and insight information security architecture particularly for information infrastructure gaps from the literature reviews, discussion with different experts working on area and also different security reports which was conducted by INSA on banking industry is an input for this research. The importance of the problem is that currently the greatest problem arisen from security breaches.

The motive of this study is to protect organizations from cyber-crime as it is extremely growing. This study develops multi-tiered security architecture towards information infrastructure protection for National bank of Ethiopia. The applicability of the proposed architecture will secure banking industry.

3.2.2 Objective of The Solution

The second step in design science is to define the objectives for an answer. The target of the answer artifact relies on the matter statement and it maybe quantitative (advancement of existing artifacts) and qualitative (new artifact for brand spanking new solution). The final goal of this study is going to develop multi-tiered security architecture for national bank of Ethiopia to confirm IIP in order to protect from cyber-attacks.

3.2.3 Design and Development

The third step is to design and develop the artifact. This step is the place where the actual artifacts (security architecture) was developed. To develop security architecture, it is imperative to look at the current practice of organization on security breaches. For this study Farah (2005) information security architecture is adopted. The functionality of this developed security architecture will secure the organizations information from any thefts. The design and development solution use identified gaps from the current practice and map with the literature reviews so that this was taken as an input to develop security architecture. Th data that was collected, by using questionnaire, interview, network traffic analysis tool and observation from the National Bank of Ethiopia.

3.2.3.1 Population and Sampling

Target Population

As the scope of this study covers Information System Management Directorate of National Bank of Ethiopia, the employees under this directorates are the total population of the research, which covers 100 in number.

Sampling Technique

Sampling is the process of taking a representative, obviously smaller size, from the population, which can approximately reflect the characteristics of the whole population so as to make the research more manageable and to be conducted in a resource effective way. There are two types of sampling techniques the probability sampling (all are equal chance of being selected) and non-probability sampling, where not all members have equal chance of being selected. For questionnaire respondents of this study the researcher has employed stratified random sampling which is more appropriate to select sample population because The ISM directorate is organized in different Teams with approximately equal in size in each stratum. For selecting interviewee researcher adopted the purposive sampling technique in order to identify key participants within the ISM Directorate who are responsible for managing the design, implementation and operations of the network and systems at a higher level.

Sampling Size Determination

The information system management directorate has four teams which include security team, network infrastructure and system team, database team and application team. All team are equal number of employees approximately 25- 30 employees. So, the total population of the study is the number of information system management directorates which is 100 staffs. For this research study Yamane's formula was adopted to calculate sampling with the consideration of 95% confidence interval and p=0.5 (Yamane, 1967).

where N= population of the study

e =(MoE) Margin of error, e = 0.05

N=100

n = N / (1 + Ne^2)

The sample size $n = \frac{100}{1 + 100(0.05^2)} = 80$

Qualitative Sampling

Purposive sampling gives an opportunity for a researcher to know key informants to acquire the required information. For this study five key informants were interviewed as it is believed by the researcher that it provides complete information.

3.2.3.2 Data Collection Methods and Procedure

As the objective of this study is to develop multi-tiered security architecture for National Bank of Ethiopia the researcher was used two basic data sources, such as existing literatures in the area of the study and data from the current practices of the company on the phenomena. Multiple data collection instruments were used in this study to increase the quality of data.

The data that was collected by survey questionnaire and interview with the support of observation and network traffic analysis tool were used to identify gaps.

Questionnaire

The questionnaire is one of the main tools used to collect a primary data and it provide data for the researcher. This questionnaire is aimed at measuring the current experience by gathering the straight forward information that are clear and unambiguous. For this study the questionnaires are adopted from the related literature reviews with modification and additions. The questioners have both background information and relevant information and are detailed information with the goal of assessing current practices on information security issues. The questioners were adopted from George Farah (2005) and the questionnaires were pilot tested by 10 users.

As a primary data collection tool, the Questionnaire consisted of 46 Likert scale questions, where the meanings of the options are indicated in table 3.1 below, and question items are categorized in General question, VPN and Proxy related question, Switch and Router question, Firewall and check point question.

Options Clarification	
Options	**Meaning**
Strongly Disagree	**Not presented or practiced in the organization at all**
Disagree	**The organization is performed or practiced**

Neutral	Does not have the information or no certainty about it
Agree	The organization is performed or practiced in some level
Strongly Agree	The organization is performed or practiced it fully

Table 3.1 Likert scale option meanings

Interview

Interview is One of the best techniques to collect data for qualitative study by providing different views and opinions of participants without any restriction. In this study semi-structure interview were employed which were based on the willing, knowledge and experience of the interviewee (John W. Creswell ,2013). It is also valuable for finding out people's motivations, and their rationale as to why they did certain things (Myers,2007). Interviews with practitioners and experts in the field can be conducted to identify relevant and addressed problems (P. Offermann et al.,2007). The interview questions were aimed to address management, police, and compliance issues. On this research five peoples were interviewed (director, chief network infrastructure Officer, chief data base Officer, chief application Officer and chief security Officer) and the whole session of the interview were recorded with the full agreement of each participant and the due consideration of all the ethical promises. The interview schedule was based on the interests of interviewee and interview were held in each interviewee's office, as the place was ideal to hold such an activity.

Participants No	Participant code	Membership
1	Participant1	Director
2	Participant2	Chief X Officer
3	Participant3	Chief X Officer
4	Participant4	Chief X Officer
5	Participant5	Chief X Officer

Table 3.2 Interviewees

Observation

Observation is a method where the researcher is entirely involved and becomes a participant in the culture of being observed (J. Collis and R. Hussey,2009). In this study, a participant observation technique is adopted as the researcher is an insider, observed security architecture which was implemented in the bank.

The network Traffic analysis tool

The network traffic analysis tools were employed to analyzed the threats of the communication network and systems by using the alien vault Open Source Security Information Management (OSSIM). The alien vault OSSIM is one of the security information and event management tools which is an open source that provides complete correlation, normalization and event collection with a feature-rich open source security information and event management. It provided a unified platform with many security capabilities like: Vulnerability assessment, Asset discovery, Security information and event management (SIEM) event correlation, Behavioral monitoring and Intrusion detection by allowing users to both contribute and receive real-time information about malicious devices, systems and hosts. In this research alien vault OSSIM is used for network traffic analysis by identifying devices, systems and database vulnerability.

3.2.3.3 Methods of Data Analysis

For quantitative data SPSS was used to analyze the data. For qualitative data thematic content analysis was used to identifies common themes in a text provided for analysis by classification and categorization. The output of both qualitative and quantitative were mapped to the literature (Anderson, 2007).

Reliability

The dealings of reliability are used to measure the quality of the research. Reliability is used to measure the consistency of the survey (Hair et al., 2014). Reliability is one of the most important criteria for ensuring a research to be highly qualified research and it shows all activity performed in the study which can be repeated with the same result (Yin ,2014). For the sake of increasing this study's reliability and to decrease the possible biases the application of multiple methods like questionnaire, semi-structured interview, observation and network traffic analysis tool were used in this study to achieve the triangulation and also Cron batch is used to measure reliability

to measure internal consistency with the result greater than 0.70 which are minimal alpha value to prove internal consistency.

Validity

Validity is used to measure the degree to which a scale or set of measures accurately represents the construct. The validity of design research must be based on the evaluation of developed artifacts (Pries-Heje and Baskerville ,2008). During the evaluation of the developed artifacts it should satisfy the need to achieve the objective of the study and accomplish their function (Pries-Heje and Baskerville ,2008). Validity is also the important factor to support practical implication of a research but some of validation methods are lacks sufficient empirical foundation (Chakrabarti ,2010). Validity is characterized by set of procedures use help to conclude the research (Mentzer and Flint, 1997). As this study employed design science paradigm and Peffes et al. (2007) design science research methodology it used the procedure that generate results by artifacts from internal design environment and external designed environment for which it is developed. To increase validity of the research the researcher employed different data collection instruments and the research must be free from any emotion and reaction and it is good for a researcher to allow respondents open mindedly. For this study the researcher was scheduled based on the interest of interviewee and the transcribed data were sent to interviewee to avoid any bias.

Pilot Testing

A pilot study has conducted to identify the problems and avoid bias on the questionnaire so that it is free from ambiguity. It was distributed to 10 users which are selected from all department of Information system directorate of NBE. The ultimate goal of pilot study is to enhance and check validity and reliability of the survey questionnaire.

3.2.4 Demonstration

The fourth design science step is to demonstrate the use of the artifact to solve one or more instances of the problem. This is the step where the identified problems were solved based on the results. The demonstration was presented to the ISMD staff who participate in questionnaire and interview process. The demonstration of the architecture was done based on the cisco packet tracer. It is performed through simulation. Therefore, the multi-tiered architecture towards

information infrastructure protection developed for national bank of Ethiopia, were demonstrated to the users to create awareness of proposed security architecture.

3.2.5 Evaluation

The fifth Design science step is to evaluate the use of the artifact to solve the problem. It is the place where the researcher should observe and measure the behavior of developed artifacts for solving the problem and if the outcome does not satisfy expectation the researcher can return to the designing and development phase to develop the new artifacts. The method of evaluation and validation can vary and can range from logical arguments to experimentation or mathematical proof in the Design Science methodology (Vaishnavi et al.,2004). Hevner (2004) propose different way of evaluating artifacts like

Observational, where it determines how the artifact is behaved and the researcher is act like an observer and does not interact directly with an environment;

Analytical, where both the performance of artifacts for internal structure and external interactions are assessed;

Testing, where the functional and structure of the artifacts are tested;

Experimental, where the experiment is controlled like laboratory and simulation;

Expert validation, where the feedback of the experts are incorporated against to the developed artifacts and

Descriptive methods, where the developed artifact utility is demonstrated. In this study expert validation will be conducted by interviewing experts on the area to evaluated developed architecture.

The first evaluation was whether the developed architecture address the problem or not and was searched for missing ideas and catch if there are new insights available for further architecture refinement.

In the second evaluation, was subjected to experts to evaluate the architecture based on the well know 'quality in use model' which is stated in the International Organization for Standardization and International Electrotechnical Commission [ISO/IEC 25010:2011] standard.

3.2.6 Communication

The final stage of design science research process is communication of the result through thesis. The communicated study employed academic literature and presented to department of information science.

According to Peffers et al. (2007), the research does not need to start from step 1 and end at step 6 but can be applied differently according to the type of the problem and the research objective and its starting point can be modified according to the goal of the research.

Chapter Summary

This chapter explained the methodological approaches that have been employed within the information systems study, and then selected a proper one for shaping and delivering the anticipated aim of the research. Accordingly, an outline of the Design Science research approach and a justification that a Design Science approach would be more desirable than other approaches are provided. The chapter also showed the type of the 'process model' used. A detailed step by step activities, based on the model, and sub-activities are also presented. Overall, the chapter was focused on presenting the activities in this research.

Chapter 4

Findings and design search process

This chapter describes the results of gathering data from questionnaire, interview, observation and network traffic analysis tools and based on the data gathered, analysis is conducted based on the findings.

4.1 Overview

As described in chapter three the design and development stage utilize findings derived from literature review, current practices of organization through interview, questionnaire, observation and network traffic analysis tools contributes to the design search process as the factor affecting multi-tiered security architecture towards information infrastructure protection which were taken as input for design an architecture. This chapter present and discusses the finding of the study which were collected from the quantitative, qualitative data, observation and network traffic analysis tool. The first section of this chapter discussed the quality of data and techniques to ensure data quality. The second section presents the quantitative data analysis. The third section discussed qualitative data analysis. The fourth section presented observation and network traffic analysis results and finally triangulation is conducted by referring the findings of quantitative analysis, observation in the qualitative discussion and vice versa.

4.2 Demographic Characteristics

From the table 4.1 the total responded participants, 36.25% are females and the rest 63.75% are males. The result shows that the majority of employees responded to the questionnaire are males which means the number of males are greater than that of female in the company. The educational status of the participants shows that all have bachelor degree and above, from which about 92.5% are bachelor degree holders and the rest 7.5% has a master's degree. This shows that the company's minimum requirement for IT related educational qualification is Bachelor degree. Regarding participant's work experience of the company, 70% worked 6 years or less, 25% have 6-10 years of service, 3.75% served 11-15 years and the rest 1.25% are served more than 15 years. This shows that the majority of the participants, 70% have work experience of less than 6 years in the company.

Gender		Education				Work experience (Year)		
Male	Female	BSC	MSC	PHD	>5	6-10	11-15	15<
63.75%	36.25%	92.5%	7.5%	0%	70%	25%	3.75%	1.25%

Table 4.1. Characteristics of respondent's demography.

The demographic data shows that the respondents are consisting from junior to senior staff members have good educational background that make them to understand survey questionnaire.

4.3 Response Rate and Data Cleaning

The questionnaire instrument used for data collection was developed for ICT employs of all network infrastructure and system, database management, application and ICT Security team. Accordingly, here below is the characteristics of respondents and the response rate.

No	Profile	Distributed Questionnaire	Returned questionnaire	Response Rate
1	ICT Staff	80	80	100 %
	Total	80	80	100%
Total	Response Rate	100%	100%	100%

Most of the respondents are located in the head office as the large number of staff is based there. The researchers have distributed the questionnaires to all respected Team in the Information System Management Directorate.

4.3.1 Data Cleaning

Data cleaning is an important way of representation for factors like missing, incorrect and inconsistence data. Identifying and correcting data error needs manual operation of data that requires cost and time (Krishnanet al., 2015).

In the data collection outliers and missing values man occur which could lead to compromise the reliability of the study (KyuKwak and HaeKim,2017). In this this study 4 missing values were identified and managed by imputation approach which is one of the ways of replacing the missing values with the mean of that variable by computing the average of the given variable.

4.4 Quantitative data analysis results and discussion

Based on the distributed questions the respondent feedbacks are presented below. There are 46 Likert scale questions used for data analysis. To fill the missing data the mean of the respondents score was used (Joshi et al., 2015).

4.4.1 Security assessment construct measures

The survey questions under general security assessment construct measures are used to know the general security gaps and threats which have been experienced. There are 10 questions under this category which enable to evaluate whether the NBE have experienced security threats or not.

Security Assessments Questions No		StronglyDisagree	Disagree	Neutral	Agree	StronglyAgree
1	All systems are up to date with patches	13 16.25 %	41 51.25%	5 6.25%	21 26.25%	0 0%
2	All needed ports are open	3 3.75%	35 43.75%	7 8.75%	28 35%	7 8.75%
3	All needed services are open	3 3.75%	22 27.5%	18 22.5%	26 32.5%	11 13.75%
4	Firewall Rule are set analysis	0 0%	30 37.5%	27 33.75%	17 21.25%	8 10%
5	All network devices are positioned properly and correctly	5 5%	28 35%	16 20%	29 36.25%	2 2.5%
6	All secure and non-secure interfaces are identified	3 3.75%	31 38.75%	19 23.75%	26 32.5%	1 1.25%
7	History of the All device is recorded	7 8.75%	35 43.75%	17 21.25%	19 23.75%	2 2.5%
8	Device Logs are checked regularly and there is a	7 8.75%	25 31.25%	21 26.25%	27 33.75%	0 0%

	responsible body for creating and deleting accounts					
9	There is responsible body for reviewing Logs	9 11.25 %	23 28.75%	21 26.25%	26 32.5%	2 2.5%
10	There is a process of change management	11 13.75 %	27 33.75%	21 26.25%	19 23.75%	2 2.5%
	Total score	7.5%	37.12%	21.5%	29.75%	4.375%

Table 4.3. General security assessment construct question items and results

The result of this measure as shown in table 4.3 above, the majority of the respondents, 51.25% confirmed that most systems are not UpToDate with patches and 43.75% of respondent show that most needed ports are not properly opened. For services which are opened for users, 32.5% of the respondent agree that all services are opened. For The company's firewall to set analysis, 37.5% respondents disagree with firewalls set analysis and 33.75% respondents are neutral and they didn't aware about firewall set analysis. 36.25% respondents are agreed with the proper position of the layer three devices where as 35% are disagree with the proper position of the devices. All secure and non-secure interfaces are identified, 38.75% respondents are disagreed and 32.5% respondents are agreed. History of the All device is recorded, 43.75% respondents are disagreed where as 23.75% respondents are agreed. Device Logs are checked regularly and there is a responsible body for creating and deleting accounts, 33.75% agreed and 31.25% disagreed. There is responsible body for reviewing Logs, 32.5% respondents are agreed and 28.75% respondents are disagreed. There is a process of change management, 33.75% respondents are disagreed and 26.25% respondents are neutral.

4.4.2 VPN and Proxy construct measures

The survey questions under VPN and proxy related construct measures are used to know the VPN and proxy related gaps and threats which they have been experienced. There are 6 questions under this category which enable to evaluate VPN and proxy related issues.

No	VPN and Proxy related Questions					
1	The Configurations of Cisco security profiles are used by users to access the network	9 11.25% 1.25%	23 28.75%	18	29 22.5%	1 36.25%
2	Your bank has VPN and distribution implementation policy	1 1.25%	16 20%	14 17.5%	36 45.50 %	12 14.25%
3	Your bank has VPN access and controls need to be on every PC	4 5%	26 32.5%	16 20%	23 28.75%	12 15%
4	Your bank has internet policy	1 1.25%	13 16.25	10 12.5%	42 52.5%	 17.5%
5	Http traffic being scanned for antivirus	6 7.5%	16 20%	15 18.75 %	36 45.50%	5 6.25%
6	Your banks proxy has a good way to stop spam	29 36.25%	28 35%	11 13.75 %	29 36.25%	 3.75%
	Total score	10.4%	29.3%	17.5%	40.8%	9. 7%

Table 4.4. VPN and proxy related construct question items and results

The result of this measure shows in table 4.4 above, the majority of the respondents, 36.25% understand that most The Configurations of Cisco security profiles are used by users to access the network where as 28.75% of respondent disagree. For VPN and distribution implementation

4.4.3 **Switch and Router construct measures**

	Switch and Router related questions:	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Your organization network connection is positioned properly.	6 7.5%	25 31.25%	16 20%	30 37.5%	3 3.75%
2	All switches and routers are configured properly and a good authentication method are used.	0 0%	32 40%	6 7.5%	41 51.25%	1 1.25%
3	All polices are configured and users are authorized properly	6 7.5%	36 45 %	15 18.75%	17 21.25%	4 5%
4	All Devices Obtain an IP address once connected	3 3.75%	24 30%	6 7.5%	36 45%	11 13.75%
5	Your networks are properly monitored	7 8.75%	27 33.75%	20 25%	23 28.75%	3 3.75%

6	Vulnerabilities are scanned on monitoring devices	7 8.75%	25 31.25%	20 25%	24 30%	4 5%
7	All networks are properly routed	3 3.75%	26 32.5%	16 20%	34 42.5%	1 1.25%
8	A good layout of cabling and devices for LAN and standard cables are used	10 12.5%	31 38.75%	17 21.25%	18 22.5%	4 5%
9	Banks has good network topology	4 5%	34 42.5%	12 15%	24 30%	6 7.5%
10	Industry standard routers, hubs and switches are used and properly changed when outdated	4 5%	39 48.75	19 23.75%	12 15%	6 7.5%
11	Change managements are used when changing routers or switch configurations	5 6.25%	39 48.75%	19 23.75%	12 15%	5 6.25%
12	Your bank has a good policy to connect any network devices to your LAN and activating switch ports	7 8.75%	34 42.5%	14 17.5%	24 30%	1 1.25%
13	physical space is accessed by granted user only	6 7.5%	34 38.75%	11 13.75%	26 32.5%	6 7.5%
14	Have policy for connecting external vendors to the LAN	5 6.25%	32 40%	22 27.5%	20 25%	1 1.25%

15	Physical security practiced properly for accessing premises and process for activating and deactivating badges, LAN ports and LAN connection drops.	5 6.25%	34 42.5%	17 21.25%	24 30%	0 0%
	Total score 6.50%		36%	19.00%	30%	4.70%

Table 4.5. switch and router construct question items and results

The result of this measure shows in table 4.5 above, the organization network connection is positioned properly,37.5% respondents confirmed that network devices are positioned properly whereas 31.25% respondents are disagreed with the position of the network devices. For proper switches and routers configuration and a good authentication method are used, 51.25% of the respondent agree that all the configuration of switch and routers by using a good authentication method. For polices are configured and users are authorized properly, 45.5% respondents disagree with configured polices and authorization of user properly. The Devices Obtain an IP address once connected, 45%respondents are agreed that devices are obtained IP addresses once connected. For networks are properly monitored,33.75%respondents are disagreed with the monitoring of the networks. For Vulnerabilities are scanned on monitoring devices,31.25% disagreed but 30% respondents are agreed with the scanning of vulnerabilities. For networks are properly routed,42.5% respondents are confirmed that all networks are properly routed. For A good layout of cabling and devices for LAN and standard cables are used,38.75% respondents are disagreed with the physical layout of the device and cable. For Banks has good network topology, 42.5% respondents are disagreed with the topology. For Industry standard routers, hubs and switches are used and properly changed when outdated,48.75 respondents are disagreed with the properly changed outdated devices. For Change managements are used when changing routers or switch configurations, 48.75% respondents are disagreed with the change management. For bank has a good policy to connect any network devices to your LAN and activating switch ports,42.5% respondents are disagreed with the device connected police. For physical space is accessed by granted user only,38.75% disagreed with physical grated policy.

For policy for connecting external vendors to the LAN,38.75% disagreed with the policy for connecting external vender. For Physical security practiced properly for accessing premises and process for activating and deactivating badges, LAN ports and LAN connection drops, 42.5% disagreed with the budgets of activating and deactivating physical security.

4.4.4 Firewall and check point construct measures

The survey questions under Firewall and check points construct measures are used to know the Firewall and check points related gaps and threats which they have been experienced. There are 5 questions under this category which enable to evaluate Firewall and check points related issues.

No	Firewall and check point Questions	Strongly Disagree	Disagree	Neutral	Agree	StronglyAgree
1	Firewall and check point positioned properly	4 5%	32 40%	19 23.75%	20 25%	5 6.25%
2	Firewall and check point have software updates and attack signatures	5 6.25%	37 46.25%	21 26.25%	15 18.75%	2 2.5%
3	All traffic that are coming to your DMZ or external and internal network are Understand and detect.	3 3.75%	36 45%	14 17.5%	24 30%	3 3.75%
4	The device has been positioned in different places on the network to understand the type of traffic that can be detected	4 5%	36 45.50%	14 17.5%	24 30%	0 0%
5	Firewall and check point configured properly and send an alarm to network administrator.	7 8.75%	42 52.5%	12 15%	14 17.5%	5 6.25%
	Total score	5.75%	45.85%	20%	24.25%	3.75%

Table 4.6. firewall and checkpoint construct question items and results

For Firewall and check point positioned properly,40% respondents are disagreed with the properly position of firewall and check points. Firewall and check point have software updates

and attack signatures, 46.25% respondents are disagreed with update of software for firewall and checkpoints. For traffic that are coming to your DMZ or external and internal network are Understand and detect, 45% respondents are disagreed with the detecting traffic of DMZ zone. For The device has been positioned in different places on the network to understand the type of traffic that can be detected,45.5% respondents are disagreed with devices detecting different traffics. The Firewall and check point configured properly and send an alarm to network administrator,52.5% respondents are disagreed with the firewalls and checkpoints to send alarms to network administrator.

Qualitative Data Analysis

This study was backed by a qualitative study beside the quantitative investigation with the main aim of enriching the study with a firm finding while triangulation was a part. In this research a more deductive approach is employed for the data analysis as the data was grouped based on the research questions to look for similarities and differences. This approach is best suited when qualitative research is a smaller component of a larger quantitative study (Sunday, 2016). Also, to avoid orphan questions a research question Vs. Interview questions matrix was used as below.

No	Interview Questions	R1	R2	R3
1.	How Do you see information infrastructure (communication networks, associated software's and delivered services) of your banks?			
2.	Do you have any certifications that are focused on information security?			
3.	Do you have the technical know how to manage the information security systems in place?			
4.	Would you tell us your experience of monitoring the network and What threats you have observed so far?			
5.	Do you know the critical systems in your organization? What are they?			

6.	Can you confidently say your information infrastructure is effectively protected?
7.	Would you tell us the challenges you face while ensuring Information Infrastructure Protection?
8.	Would you Give us a high-level description of the information infrastructure?

Table 4. 7: Research question Vs. Interview questions matrix

Accordingly, interviews have been conducted with 5 staffs (1 director and 4 team leaders) to acquire high level information on security and information infrastructure. The questions were framed and adopted from the research which was conducted earlier on the related area. As discussed in chapter three method of data analysis section, the interview output was analyzed using thematic content analysis.

4.5 Qualitative data analysis results and discussion

The overall Qualitative Analysis process followed Creswell's steps to come up with a global theme.

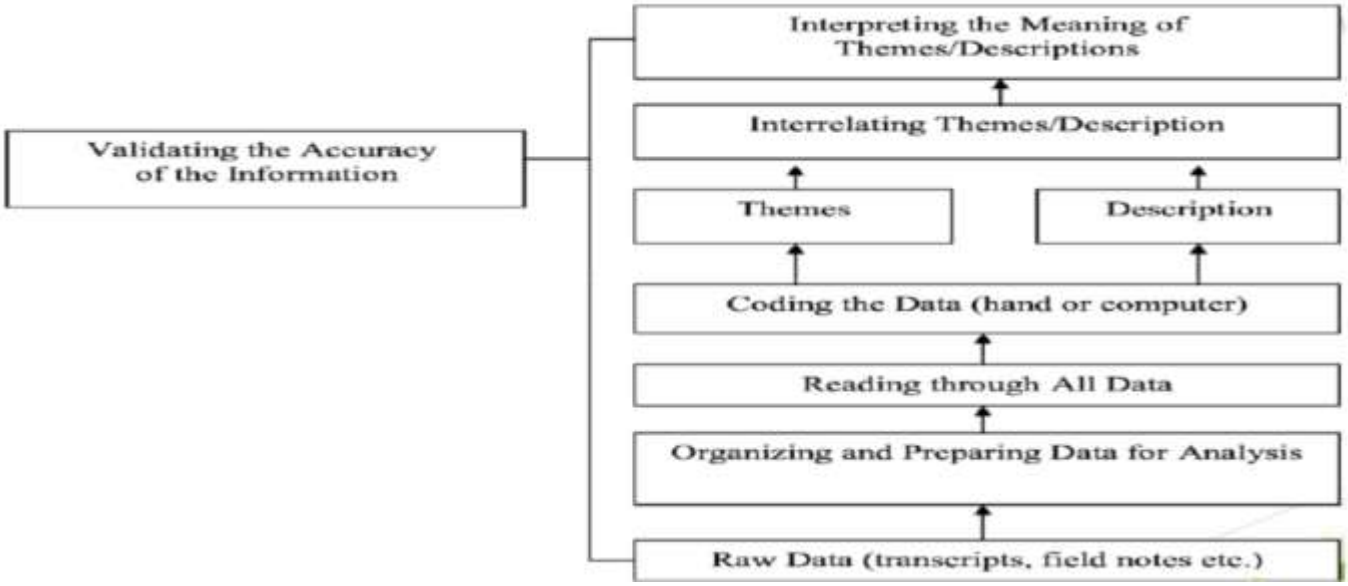


Figure 4. 1. Data Analysis steps followed in Qualitative Research adopted from (John W. Creswell, 2013) Page | 60

Accordingly, the recorded interview data was prepared and organized for analysis by typing it to notes to acquire the general information. The coding was done via labeling a word representing a category and the sample screenshot given blow.

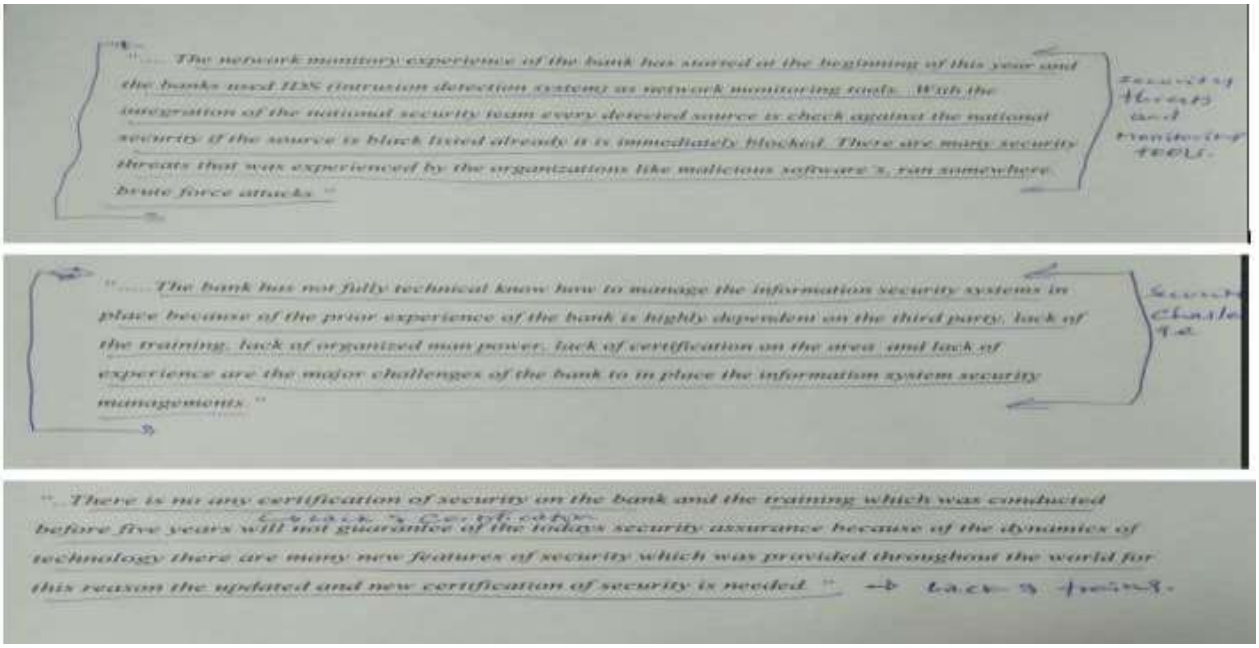


Figure 4. 2: Sample data labelling in the qualitative data analysis process

The first question presented to the interviewees was regarding the understanding of information infrastructure in terms of communication network, associated software and delivery services. The responses from the interviewee are similar on the understanding of the information infrastructure. They stated that the information infrastructure of the bank in terms of communication networks are all devices which connect users to access systems include switch, routers, checkpoints and firewalls ; associated software's include all software's like IOS(inter operating system), all servers like windows, Linux and database and deliver services are all services which are delivered by the bank include data service, internet services. In fact, one of the interviewees said "…. In the Information infrastructures there are many concepts mainly

technology, human elements and process with in this three all components such as communication networks, software's and delivered services are part of it. As communication networks the banks have all devices such as switch, router, firewalls, checkpoints. As associated software the banks have IOS which was run on that communication network hardware's and aliso Linux, windows servers for FTP, Active directory, all systems. As services the bank has

many data services such as credit information of the customer of any commercial bank, automated transfer services, collateral register services and core banking system service."

These finding show that the banks ICT Manager have an understanding on information infrastructure regarding communication network, associated software and deliver services but they lack the deep understanding and awareness of information infrastructure.

The next questions were the experience of the bank on certifications that are focused on information security. On this question all the interviewees raised similar response which shows that there is no certification which are particularly focused on the information security but there were training of security as a general. One of the respondents notes that "..There is no any certification of security on the bank and the training which was conducted before five years will not guarantee of the todays security assurance because of the dynamics of technology there are many new features of security which was provided throughout the world for this reason the updated and new certification of security is needed. "

These finding show that there is lack of training and certification on the area of security and the bank needs qualified and certified employees on security area.

The other question was the technical know how to manage the information security systems in place, on this part the response of the respondents is there are lack of training and experience on managing information security and there are also open source systems to manage incidents. So, all respondents are responded that there is no fully technical capability to manage information security systems. One of the respondents said that "…..The bank has not fully technical know how to manage the information security systems in place because of the prior experience of the bank is highly dependent on the third party, lack of the training, lack of organized man power, lack of certification on the area and lack of experience are the major challenges of the bank to in place the information system security managements."

The next question deals with that experience of monitoring the network and What threats you have observed so far, all respondents are noting the similar feedbacks by stating that the bank has not long time experience the monitoring of the network were started in the beginning of this very year after the incidents was happened on the bank and the most observed attacks are brute force attacks which aimed to know the identity of a user and malicious attacks like virus, trojan

horse, ran somewhere and worms. One of the respondents notes that "…. The network monitory experience of the bank has started before year and the banks used IDS (intrusion detection system) as network monitoring tools. With the integration of the national security team every detected source is check against the national security if the source is black listed already it is immediately blocked. There are many security threats that was experienced by the organizations like malicious software's, ran somewhere, brute force attacks."

The other question deals with the critical systems of the organization. All respondents have reflected the similar feedbacks on this question. Yes, the bank has critical systems and the critical systems are credit information system (CIC), Ethiopian automated transfer system (EATS), core banking (QBS), Collateral register system, swift system and routers system. One of the respondents notes that "To have financial stability the bank has credit information system the most critical one where any commercial banks are making sure about their borrowers' history before they lend money to them and also Ethiopian automated transfer system also critical where the exchange of money is monitored. The other critical systems are core banking system which allow the bank to properly manage the income and expenses."

The other question is Can you confidently say your information infrastructure is effectively protected. On this question all the respondents are different understanding on the way of measurement to be protected fully some said it is partially protected and other said it is fully protected. One of the respondent's notes "The network is expected to be secured 100% and till now there is no such big challenge which compromise our security and we feel that we are protected fully. The awareness of the top managements is main problem on making the decision regarding the security."

"……. The other interviewee noted that the network of the bank is 75% protected. there are inside compromises because users are sharing passwords, there are not full patch updates of system, the durability of devices are low are among main reasons which open hole for threats"

Other question deal with the challenges face while ensuring Information Infrastructure Protection, all respondents are similar response on this question. The most common challenges are lack of training, lack of top management support, lack of experience, lack of commitment, lack of user awareness, the flexibility of security nature. One of the respondent's notes "…….

The common challenges of information infrastructure are lack of top management support, lack

good project management approach, lack of commitment, lack of awareness, lack of training are the common challenges for information infrastructure protection. "

The final question deal with a high-level description of the information infrastructure. Based on their understanding the describe information infrastructure as hardware and software's. The hardware includes all communication network devices like switch, router, firewalls, checkpoints. Software are all IOS, Microsoft servers and Linux. One of the respondent's notes "……

information infrastructures are defined in the way of the three pillars like technology (hardware and software), peoples and processes so these three components are working to gather to achieve a good information infrastructure protection."

4.6 Network traffic analysis and Observation

Additional instrument of network traffic analysis and observations are used with aim of strengthening and supporting the survey and interview instruments. The network analysis is with the consideration with banks security policy. The researcher observes several network analyses results in several times.

4.6.1 The network and system traffic analysis result using Alien Vault OSSIM

The alien vault OSSIM is one of the security information and event management tools which are an open source that provides complete correlation, normalization and event collection with a feature-rich open source security information and event management. It was launched be security engineers specifically to address security control mechanism for many securities professionals for security visibilities. It also proves unified platform with many security capabilities like: Vulnerability assessment, Asset discovery, SIEM event correlation, Behavioral monitoring and Intrusion detection by allowing users to both contribute and receive real-time information about malicious devices, systems and hosts.

According to the analysis the following results were noted for confidentiality purpose systems are labeled by system 1,2,3….

Systems	Number of vulnerabilities on day one	Number of vulnerabilities on day two	Number of vulnerabilities on day three
System 1	688	633	633
System 2	66	55	55
System 3	103	103	103

System 4	66	66	66
System 5	55	62	62
System 6	48	54	54

Table 4.8: network analysis results

Factors affecting multi-tiered security architecture towards IIP

The finding of questionnaire and interview address the first research question which indicates factors affecting multi-tiered security architecture towards IIP. The evaluation finds the gap in security architecture towards information infrastructure protection. Factors affecting multi-tiered security architecture towards information infrastructure protection are presented below. Factors Affecting multi-tiered security architecture towards IIP from quantitative analysis After the questionnaire were conducted the followings are the identified factors which affecting security architecture towards IIP for banking industry.

Not All systems are up to date with patches regularly

Firewalls are not fully set analysis based on rule

Most device interfaces are not identified as secure and non-secure. Absence of regular antivirus installation and updates

Lack of good network monitoring system.

Lack of strategy on security architectures

Lack of organization of recorded device history.

There is lack process of change management

Lack a good authentication method for devices.

Lack of comprehensive polices to properly changed network devices when outdated. The overall assessment of the bank show that:

Most system is hardened and is up to date.

The existing firewalls need to be upgraded

The firewalls do not have capability to protect web server and databases attacks.

Factors Affecting multi-tiered security architecture towards IIP from qualitative analysis

The interview data analysis show that the followings are factors which affect multi-tiered security architecture towards information infrastructure for banking industry.

Staffs have Lack of skills on the area

security Lack of top management support

Lack of staff commitment

Lack of standard certification on the area of security.

There are challenges of technical know how to manage the information security systems in place.

There are inside and outside threats which are experienced by the banks.

Chapter summary

This chapter was mainly focused on the presentation and interpretation of the data findings, which was accomplished via different techniques. Survey questionnaire mainly, with the support of interview, network traffic analysis and observation were employed for data collection. Survey questionnaire was intended to acquire the views of section managers and employees under their work unit, whereas the interview was aiming to address the company's plan and current practice, security architectures, with middle and senior level management members. The network traffic analysis and observation part are targeting on presenting a supportive information, for any purpose, finding new insights, and for strengthening the findings for the understanding of the current practice of the organization's security architecture development.

Chapter 5

Architecture development and description

5.1 Overview

The objective of this study was to build a security architecture which ensure information infrastructure protection for national bank of Ethiopian. The architecture development is based on the consultation of the available literatures on the area of the study and by the assessment result of current security related practices. The assessment results of the survey questionnaire, interview, and network traffic analysis with observation are used for identifying the gap, need, and recommendations of the company and to formulate requirements for architecture development.

5.2 Current Bank Architectures

The current security architecture of information infrastructure of the bank is represented diagrammatically. The bank has connection with the all commercial banks, all microfinances, all lease companies, Ethiopian Commodity exchange (ECX), Ethiopian road authority (ERA), Ethiopian revenue custom authority (ERCA) and Ministry of Finance and Economic Development (MOFED) throughout the country. The current security architecture shows that all systems that operate and deliver the expected services helps to understand the gap of the current architecture and leads to design new architecture which ensure the protection of information infrastructure.

There are two layers of connections which were terminated on the internet routers for internet services and edge router for data services. The configurations are done for incoming and outgoing traffics. The next connections are internet routers which are terminated to external firewalls where access lists rules are configured to allow and deny traffics. From the network traffic analysis result show that most attacks are bypassed external firewalls which indicate that it cannot able to detect attacks and violations as it is first line of defense. Then the external firewalls are terminating connection with DMZ switches where internet accessible services are placed like web servers and users access web servers are not allowed to access internal LAN which are protected by internal firewalls. The DMZ switches are terminated connection with core switches which are the backbone for all networks and directly connected with distribution switches that distribute network to access switches. The internal firewalls are responsible to

protect attacks with the regular patch updates and update with new IOS. The layer access switches are connected to the distribution switches which have Virtual Local Area Networks (VLANs) configured with IP subnet in its own VLAN. The uses of VLANS are to segment networks which enable administrators to easily identify and manage networks.

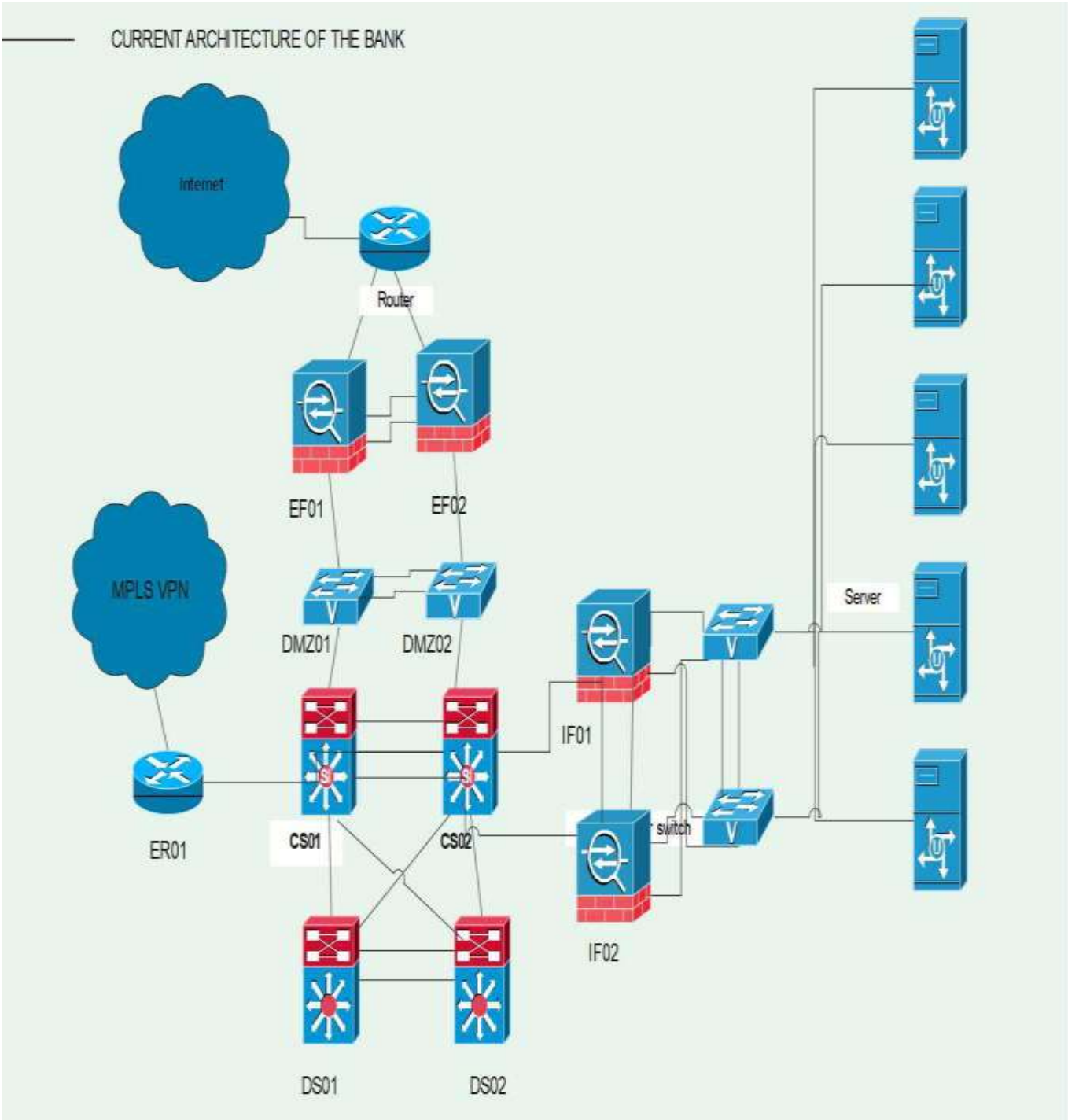
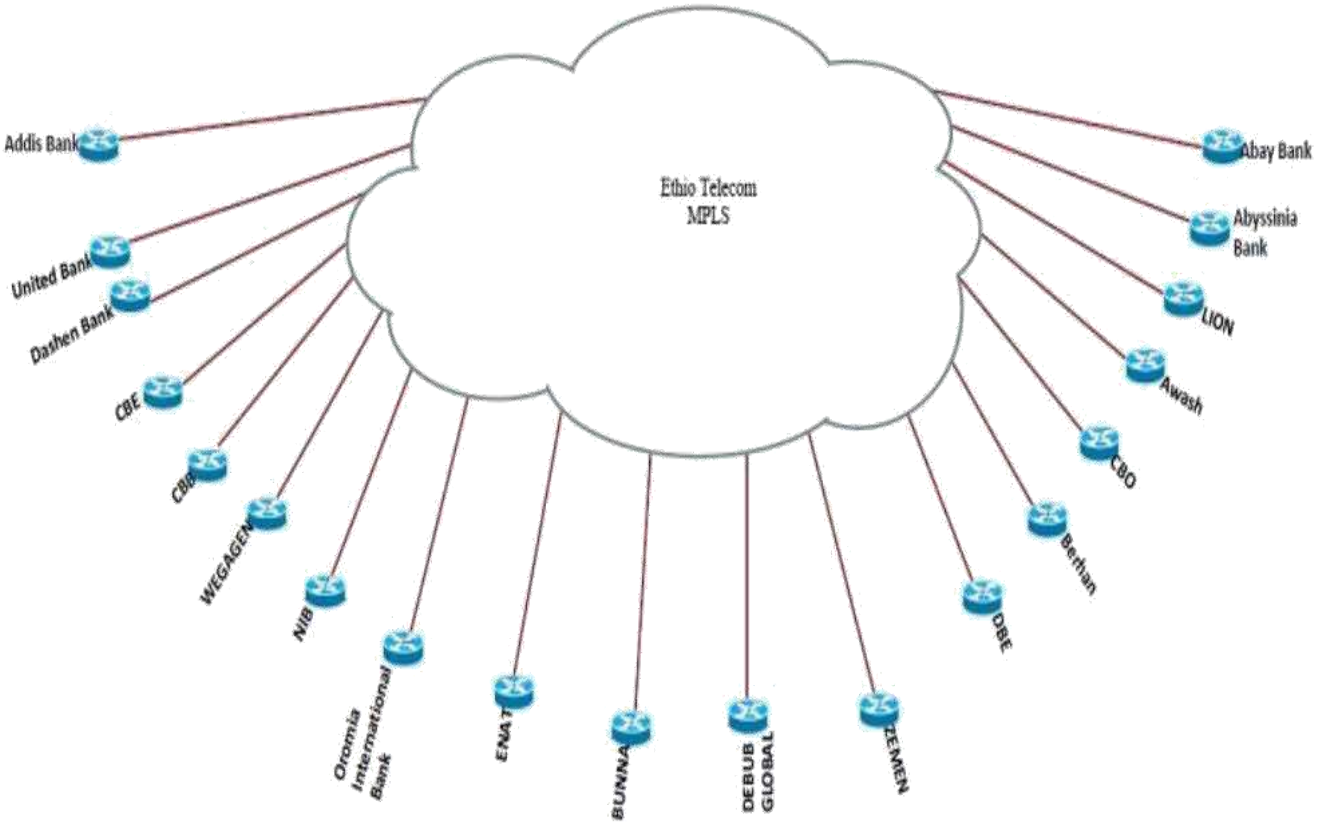


Figure 5.1: Existing NBE Network Logical Topology



5.2 Ethiopian commercial banks connection with Ethio-telecom multiprotocol label switch (MPLS) VPN connection.

5.2.1 Challenges of existing architectures of the bank

As it is strongly noted on the process of interview and questionnaire all respondents have agreed on the need of improve the existing information infrastructure to secure the banks system from threats. All interviews are assuming that traditional firewalls are strong enough to protect all information infrastructure of banks which are against the popular belief that traditional firewalls are not able to detect database and web servers so in this case it is highly vulnerable to the attacks which targeted web database and servers. The other challenges are most security devices are out of sale which has its own problem to offers security services. So, this study also proposes the new security devices to secure the information infrastructure of the bank.

The traditional firewalls are not strong enough to inspect http requests to maintain web access signature to protect web servers from any cyber-attacks. Also, traditional firewalls have no ability to carry database audits based on different operation of databases. To protect web servers

and databases the study proposed WAF and DBF. The web application firewall is a security technology which have a predefined rule and allow to configured local police which is used to allow or deny based on the criteria. It is based on the http request, response and number of occurrences. The local police are configured to match the signature and based on the result the rule is applied. The database firewall is a security technology which is able to audit the database by using preconfigured database polices. It manages the creation of tables that are critical for the business so that when the table is inserted, modified or deleted it gives an alert. The traditional firewalls must be replaced by the next generation firewalls which have Intrusion Prevention Systems to protect advanced cyber-attacks.

Check point firewalls are also proposed on the new security architecture. Check points firewalls are a security technology which are able to control the traffic to and from internal or external networks by enabling network administrators to control access of applications and servers. It has a rule which are designed to authorized connections and prevents vulnerabilities in a network, gives access to authorized users, optimizes network performance and efficiently inspects connections. The Check Point Threat Prevention solution have powerful security features such as firewall, IPS, Anti-Bot, Antivirus, Application Control, and URL Filtering to combat known cyber-attacks and threats. Also, it gives an absolute in-depth visibility.

5.3 Artifact design process

The ultimate goal of this activity is to provide an architecture, which requires the application of the rigorous method in both construction and evaluation of the designed architecture. According to the Hevner et al. (2004) the rigor for construction activity is assessed with the applicability and generalizability of the designed artifacts. Also, Johannesson and Perjons (2014), stated that creative methods are more important and brainstorming and participative modelling were used. The following approach were used to design the security architecture

1. **Factors affecting multi-tiered security architecture towards information infrastructure were identified from analysis of the quantitative, qualitative findings, network traffic analysis result and observation.**
2. **These factors were taken as an input for first draft architecture design.**

3. As participative modeling was the approach for the architecture design, multiple brainstorming session was created with the interview participants to amend the design.

4. Re-design was done to incorporate the feedbacks.

5. Finally, the architecture design layout/looks followed George Farah (2004) architecture design used to security architecture design.

5.4 Proposed Artifact

Prior to discussing the proposed architecture, it is essential to define what an architecture is. An architecture is the conceptual structure and logical organization of a computer or computer-based system. It must be Layered and is a metaphor derived from building trade like the homeowner designing a home, information technology professionals provide architectural drawing for enterprises information system and processes. (Harmon P.,2002; DeLooze LL,2001; Heaney J et al.,2002, Harjinder S.,2010).

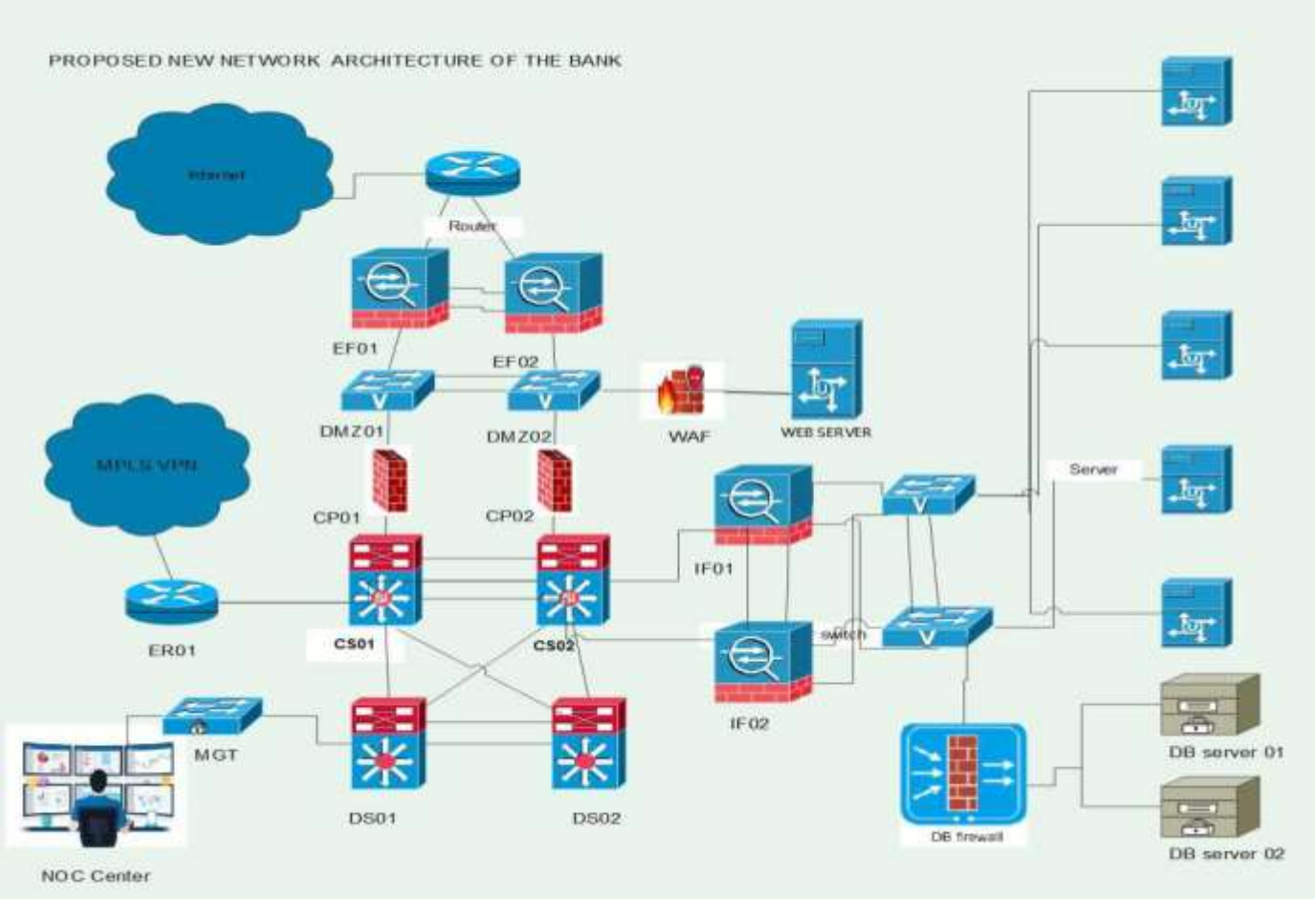


Figure 5.3: proposed NBE Network Logical Topology

Different types of architecture under the area of information system such as: network architecture, computer architecture, system architecture, software architecture, information architecture and security architecture (Edward A., 1999; David Garlan & Mary Shaw,1993; Harjinder S. ,2010; D. Comer, 2005). Accordingly, the proposed architecture is security architecture on the scope of information infrastructure, the designed architecture tries to address information infrastructure protection.

The new architecture has checkpoints, web application firewalls and data application firewalls. Check points are able to protect any attacks which are aimed to harm internal network of the company. It is a capable to protect any violations and attacks from any sources. These checkpoints are placed between DMZ and Core switches so that customer can access companies' website but cannot be allowed other systems like core banking, EATS, CIC etc. Web application firewalls are a firewall which protect web servers from any threats and all traffics must go through WAF before accessed web servers. This shows that the traffics are inspected and permitted before go to web server. The other one is database application firewall (DAF) which are responsible to protect databases from any violations. It protects database from database targeted attacks. All connection must go through database application firewalls before accessing databases.

5.5 Demonstration and Evaluation of the proposed architecture

Demonstration and evaluation are one of the integral parts of DSRM of designed artifacts. Also, Hevner et al. (2004) described that demonstration is the utility, efficacy and quality of developed artifacts. The demonstration of the artifacts is the way of solving the problem through experimentation, case study, simulation. Whereas the evaluation of the artifacts is the capability of the designed artifacts to solve problems solution (Peffers et al., 2007).

That below figure 5.4 describes the demonstration of the architecture of the bank by using simulation software. The functionality, completeness, consistency, accuracy, performance, reliability, usability and fit with the organization and other relevant quality attributes of a good designed artifacts. There developed security architecture are presented to the staffs who were participated in questionnaire and interview. the expert interview was conducted based on the experience of the expert on the area.

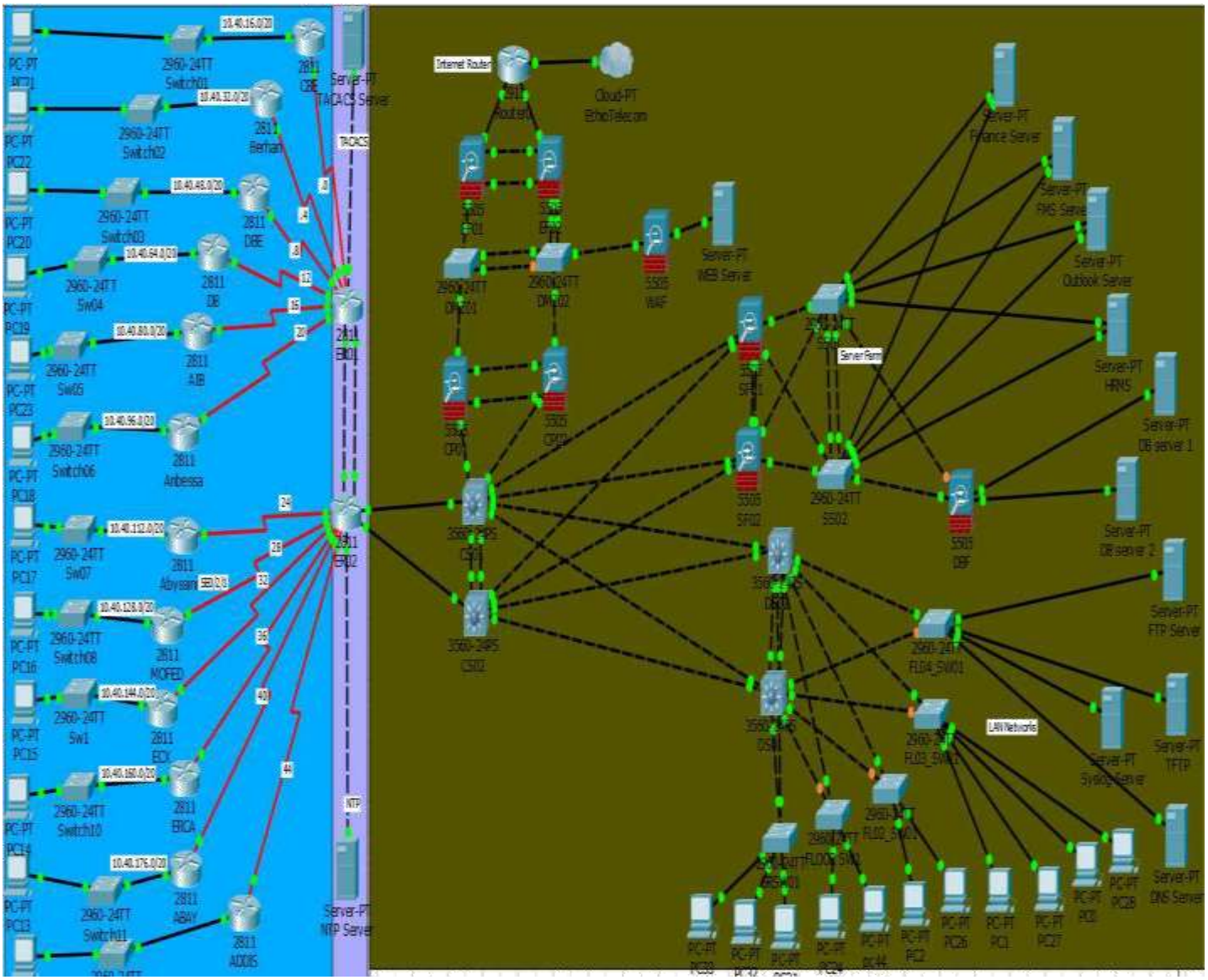


Figure 5.4: Demonstration of architecture by using packet tracer simulation

5.6.1 Architecture validation procedure using expert interview

The expert interviews are conducted by elaborating the statement of the problem and the detail of designed security architectures so that the experts are clear understanding on the problem and proposed architecture in the form of picture. If the experts are any question regarding problem and proposed architecture it is open for them to ask and if they are clear then the interview is conducted for verifying content, utility and applicability of the Architecture of designed architecture for stated problem.

To evaluate the developed security architecture interview was conducted. It was carried out on the security experts from internal and external organizations to achieve the protection of

information infrastructure. The followings are the expert interview feed backs on security architecture.

A security expert from exper1 show that the separation of internal and external networks was very important. The concept brought out in the architecture where all traffic internal and external is treated as untrusted and therefore has to be scanned before forwarding to the desired destination is very important in ensuring information security. A point to highlight was that all network firewall should be next generation firewalls (NGFW) as opposed to traditional firewalls. This is because NGFW's have better detection mechanisms including intrusion prevention system and detection of web attacks thus offering better security than the traditional firewall. However, it was their proposal that there be two sets of firewalls on for the internet edge and another for the external edge which should manage all user access to local resources within the organization. It also proposed wireless access point and wireless controller in order to manage all wires networks. To manage all mobile device the expert also recommended mobile device management to manage all wireless traffic.

A security expert from expert 02 show that the architecture generally was good for infrastructure protection. However, it was highlighted that is would be important to have a redundancy to reduce single point of failure as this will improve availability. It was also proposed that internal communication to servers should also be inspected as this will help deal with insider attacks as there will be visibility of user actions. This means introduction of an internal firewall. It was also proposed that server to server communication also be inspected as well but after careful consideration of any latencies that may be introduced due to forwarding all communication to the firewall first.

A security expert from exper03 show that the web application firewall and the database firewall are an important aspect in securing information and also the load balance was emphasized to ensure the availability of service. It was recommended that software-defined networking (SDN) architecture is easily manage the organizations information infrastructure than traditional safe architecture which are manual and static to configure and manage devices.

A security expert from exper04 show that, the proposed architecture was good for information infrastructure protection. The Web Application Firewall is very important in securing web applications which has granular policies, dynamic application profiling, threat intelligence and

report generation. The Data Base Firewall is able to classify and identify sensitive data to secure databases. The expert suggested integration of a Security Information and Event Management (SIEM) solution. This is important for easy visibility of the organization's infrastructure security. The SIEM enables one to view all relevant data from a single point by collecting logs and security information from various devices. This makes it easy to identify issues and incidences.

5.6.2 Architecture validation procedure using Evaluation survey

The survey evaluation is adapted from Paulin (2017) as stated on attached Appendix C. the respondents are selected purposively according to the experience they have on the area. The evaluation on this questionnaire helps to assure the utility, contents and application of the designed architecture. There are eight respondents for this questionnaire. The results are analyzed as follow.

6.2.1 Evaluation result of the proposed architecture

Cronbach's alpha reliability test is conducted to evaluate the consistency of the survey and the value of Cronbach's Alpha is 0.820 which indicate the reliability of the survey greater than 0.7 as showed in table 5.2.

Reliability Statistics

N of Items	11
Cronbach's Alpha	.820

Table 5.1 Reliability Statistics

Here below the reliability statics for questionnaire evaluation. The mean vales are greater than for which show that the respondents are strong agreement on utility, application and contents of designed architecture. The mean of mean is 4.5 which is very good.

Descriptive Statistics

	Descriptive Statistics	N	MIN	MAX	MEAN	STD.DEV
	The presentation of the architecture being in a suitable manner, its comprehensibility and coverage					
1	The Developed security architecture is understandable.	10	4.00	5.00	4.07	.302
2	The Developed security architecture is comprehensive in terms of coverage.	10	4.00	5.00	4.09	.302
3	The organization and presentation of the security architecture is suitable.	10	4.00	5.00	4.45	.522
4	The objectives of four imperatives (Strategic, Tactical, Operational & continuous improvement) is comprehendible.	10	4.00	5.00	4.55	.522
5	The objective of the architecture is comprehensible.	10	4.00	5.00	4.82	.405
	Regarding the content of the Architecture					
6	The contents of the Developed security architecture are clear.	10	4.00	5.00	4.82	.405
7	The contents of the Developed security architecture are correct.	10	4.00	5.00	4.91	.302
8	The contents of the Developed security architecture are complete.	10	4.00	5.00	4.91	.302
	Regarding utility and applicability of the Architecture					
9	The Developed security architecture is applicable.	10	5.00	5.00	5	0.000
10	The implementation of the Developed security architecture fits with the organization.	10	5.00	5.00	5	0.000
11	The applicability of the Developed security architecture can improve information infrastructure protection.	10	5.00	5.00	5	0.000

Table 5. 2. Mean and standard deviation of the security architecture Evaluation Survey (Evaluation criteria adapted From Pauline (2017) based on Hevner et al. (2007) evaluation guidelines.

According to the evaluation result, the utility and applicability of the architecture has the highest aggregate mean value of 5 indicating that the respondents agree the architecture is applicable, fits the organization and can ensure information infrastructure protection. The content architecture scored second high aggregate mean value of 4.88 which demonstrates respondent's

strong agreement on this matter. By comparison the presentation of the architecture being in a suitable manner, its comprehensibility and coverage scored 4.37 suggesting possible areas of improvement to ensure its completeness.

5.6.2.2 Evaluation of the architecture against other architecture

As it is described on the statements of the problems and related work section Pauline (2017) come up with security architecture towards information infrastructure protection for Kenyan commercial banks. This architecture is identifying the challenges of the bank which affects information infrastructure protection and the security architecture were proposed. As the architecture were context dependent this architecture cannot be applicable for Ethiopian banks. The other problem of the architecture is the researcher used explorative research study to develop architecture while architecture developments are the main part of design science. There are also factors which are identified for security architecture towards information infrastructure protection like the awareness, policy, commitment, management support and staff training which are also different from one country to another as it depends on organizational cultures.

Chapter Summer

To ensure confidentiality, integrity and availability the designed security architectures are a high capability to block and attacks which will be from any direction. The devices which are outdated like firewalls are replaced with the next generation firewalls which have advanced security features than ASA firewalls. For web server web application firewall is proposed for web security. Database firewall is proposed to secure databases which are not currently existed. The ASA firewalls are not capable to protect web services and databases.

Chapter 6

Discussion, conclusion and recommendation

The discussion, conclusion and recommendations are described on this chapter. Also, future works are addressed here.

6.1. Discussion

As interview, questionnaire, network traffic analysis identified lots of challenges for information infrastructure protection which indicated that security staffs are not fully skilled. As stated in the literature to secure information infrastructure it must be fulfill the following components include: Train staff on security policy, staff commitment, have qualified security staff, top management commitment on security related issues, have secure system development, adhere to the security policies, guarantee against losses like insurance.

The employees who manage information security must be knowledgeable and capable to fulfill their responsibility. Most organizations are assuming that traditional firewalls are strong enough to protect information infrastructure while on the reality those firewalls are not capable to protect web applications and data base attacks.

The existing security devices are not capable to protect and defend advanced security threats and without in placing security pillars it is very difficult to ensure information infrastructure of the bank. The top managements are not committed to implement and invest on security which contributes the main factors to compromise information infrastructure protection.

Designing and developing security architecture without enterprise security architectures are very challengeable because enterprise security architectures are a holistic and achieve goals of company by aligning technology with business. Implementing enterprise security architectures includes security polices, processes, requirements and justification. The implementation of security architectures is different from business process and structure so enterprise security architectures are important as described on the SABSA in the model for security architecture. The firewall is highly performed inspection of any traffic from any sources of internet connection based on the rule that have been set to be allow or block depending on the rule. A new feature firewalls are intrusion detection and intrusion prevention features which enable companies to monitor intrusions which are easily detected and blocked (Lindstrom, 2004).

Different groups are identified that web attacks are happened because of lack of access control, injections, cross site scripting, lack of encryption and lack of authentications of the organizations. To secure web servers web application firewalls are recommended to secure web applications servers which are not detected be traditional firewalls because the attackers are used different methods like session manipulation, SQL injections, cross site scripting, command injections to attack web servers. The web application firewall identifies applications in a layer which are hosted in web servers to filter web traffic in sessions, positive or negatives (Khochare & Meshram, 2012).

The Database is very critical for the banks because it contains data and information. Compromising this data is cause crisis of data corruption, modification and deletion. Databases are secured by using database firewalls (Bai & Liu, 2006).

6.2. Conclusion

Because of growing attacks from time to time continually organizations like banking industry is highly vulnerable due to sensitive data they carry for this reason the information infrastructure must be protected. Banks are loosening lots of money through cyber-attacks. The developed security architecture helps the banking industry to ensure IIP which helps to minimize the numbers of attacks on web, applications and database. The highly trained security personnel are needed with the updated systems. Because of timely changing nature of the technology, the timely trainings of the security staffs are highly important to mitigate the security threats.

To address the research questions and design the architecture the DSRM with the employ of multiple data collection procedure like questionnaire, interview, network traffic analysis and observation. This study come out with design and development security architecture. Based on literature review supports the identified areas are deeply investigated. To identify factors which affect security architecture questionnaires are distributed to four department of ICT staffs under information system management directorate. The designed security architecture pass through many processes starting from analyzing questionnaires and interviews and finally factors affecting security architectures are analyzed. This analysis is mapped to literature to produce the first level of security design. The second is conducting with interviewers to better design as participatory modeling were used. Finally, the designed architecture was evaluated with a good satisfaction. The first research question was factors affecting multi-tiered security architecture towards information architecture and the finding show that there is lack of top management

support on deciding security related decisions. The other is lack of training and certification on the area of security. Lack of commitments are the main factors which was identified from interviewers.

factors affecting multi-tiered security architecture towards information architecture protections are identified below.

- **Skill gaps**
- **Lack of staff commitment**
- **Lack of Management commitment**
- **Lack of training and certification on area of security**

To solve the identified challenges the study design and develop architecture towards information infrastructures to secure banks infrastructure. As the factors are from different dimension the developed architectures are aimed to achieve the goal. The designed architectures are aimed to protect database, application, web servers, FTP servers, active directory, exchange servers and other systems like CIC, EATS, Core banking systems. For top management gaps this study is pointing towards them to give attention for security and give decision when needed. For skills, training, commitment and certifications the banks are aware of the problem and solve the identified problem.

6.3. Recommendation

The designed security architectures are great impact on improving information infrastructure protection. The developed architectures are validated by experts through interview.

On this study factors which affect multi-tiered security architecture towards information infrastructure protection identified which helps to address the gaps and the developed architecture used to solve the problem.

The following recommendations are forwarded on securing information infrastructure of the banking industry.

> **There is practice, skill on the ICT staff side, to secure banks resource all respected staffs should equipped the required skills. So, capacity building, knowledge management and sharing should be conducted.**

The management support is needed to fully address the security because of the nature of security which is flexible.

The staff commitments are needed to monitor every network and mitigated when information infrastructure compromise is happened. Hence the company give attention and motivate staffs to be highly committed.

Some devices are out of sell which opens the hole for attackers to compromise information infrastructure of the company.

The police shall be in place to operate device per standards.

Even if there are internet polices it is compromised most of the time so the company give attention for the policy and take a measurement when compromised.

6.4 Recommendation for future work

The study addresses the major area of the security based on the previous studies. Below is the researcher's suggestion for future works.

This study developed architecture based on identified factors for future study the policy and procedures of the bank are put in place to ensure information infrastructure protection.

This study is limited on the information infrastructure for the future datacenter security both physical and logically are one of the research areas.

The architecture is ahigh-level but the architecture requires the detail guidelines. Hence developing implementation strategy is research area.

This study is conducted on central banks but commercial banks are part of research areas.

This study developed safe architecture which are conventional hardware architecture the software defined networking is research area.

The wireless network is another part of the research.

Reference

Absalom Negussie. (2015). Practices, Challenges and Prospects of Information Security in

Ethiopian Banking Industry, School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia.

Adler, M. J., & van Doren, C. (1972). How to read a book. New York: A Touchstone Book Published by Simon & Schuster.

Adnan R., Suhaimi S. and Norhayati H. (2017). Information Security Challenges: A Malaysian Context. International Journal of Academic Research in Business and Social Sciences. 7. 10.6007/IJARBSS/v7-i9/3335.

Agboola, A. (2007). Information and Communication Technology (ICT) in Banking Operations in Nigeria – An Evaluation of Recent Experiences. African Journal of Public Administration and Management, XVIII(1), 1–21.

Alemu, M., & Omer, A. M. (2014). Cloud computing security framework for banking industry. HiLCoE Journal of Computer Science and Technology, 2(1), 79-85.

Albuquerque Junior, A. E., & Santos, E. M. (2014). Adoption of Information Security measures: an analysis model for public research institutes. Brazilian Journal of Scientific Administration.

Albuquerque Junior, A. E., & Santos, E. M. (2015). Adoption of information security measures in public research institutes. Proceedings of the 12th CONTECSI International Conference on Information Systems and Technology Management. doi:10.5748/9788599693117-12contecsi/ps-3155.

Anderson, R. (2007). 'Thematic content analysis (TCA): Descriptive presentation of qualitative data', Wellknowing Consulting, pp. 1–4. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Thematic+Content+Analysis+(TCA). +Descriptive+Presentation+of+Qualitative+Data#0.

Angelo, S. M. (2001). Security Architecture Model Component Overview. SANS Institute information reading room.

Ahmad, A., Maynard, S. B., & Park, S. (2012). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25(2), 357-370. doi:10.1007/s10845-012-0683-0.

Aken, J. E. (2004). Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. Journal of Management Studies, 41(2), 219-246. doi:10.1111/j.1467-6486.2004.00430. x.

Allison, D. (2013). The Insider Threat Problem the Case of a Jamaican Government Organization.

Alves-Foss, J., Taylor, C., & Oman, P. (2004). A multi-layered approach to security in high assurance systems. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the. doi:10.1109/hicss.2004.1265709.

Amare, B. (2015). Assessment of Insider Threat in Ethiopian Banking Industry Assessment of Insider Threat In Ethiopian Banking Industry.

Ambriola, V., & Tortora, G. (1993). Advances in Software Engineering and Knowledge Engineering. Series on Software Engineering and Knowledge Engineering. doi:10.1142/2207.

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313. doi:10.1016/s0167-4048(03)00407-3.

Atkins, D. E., Droegemeier, K. K., Feldman, S. I., García Molina, H., Klein, M. L., Messerschmitt, D. G., Messina, P., Ostriker, J. P., Wright, M. H., Garcia-molina, H., Klein, M. L., Messerschmitt, D. G., Messina, P., Ostriker, J. P., & Wright, M. H. (2003). Revolutionizing Science and Engineering Through Cyberinfrastructure: Report of the National Science Foundation Blue-Ribbon Advisory Panel on Cyberinfrastructure. Science,

84. http://www.nsf.gov/od/oci/reports/atkins.pdf

Aychiluhim, D., & Tibebe, B. (2013). Internet Banking Security Framework : The case of Ethiopian Banking Industry.

Bai, K., & Liu, P. (2006). Towards Database Firewall: Mining the Damage Spreading Patterns. 2006 22nd Annual Computer Security Applications Conference (ACSAC06). doi:10.1109/acsac.2006.52.

Baharon, M. R., Shi, Q., & Llewellyn-Jones, D. (2015). A new lightweight homomorphic encryption scheme for mobile cloud computing. Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, October 2015, 618–625. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.88

Bayazit, N. (2004). Investigating Design: A Review of Forty Years of Design Research. Design Issues, 20(1), 16-29. doi:10.1162/074793604772933739.

Behling, S., Floyd, K., College, M. S., Smith, T., College, M. S., Koohang, A., & College, M. S. (2009). Managers' Perspectives on Employee Information Technology Fraud Issues Within Companies/Organizations. Issues in Information Systems, 10(2), 76–81.

Bhasin, M. (2007). Mitigating Cyber Threats To Banking Industry. The Chartered Accountant, 5(10), 1618–1624.

Bieser, J., & Hilty, L. (2018). Assessing Indirect Environmental Effects of Information and Communication Technology (ICT): A Systematic Literature Review. Sustainability, 10(8), 2662. doi:10.3390/su10082662.

Björck, F. (2005). Discovering information security management. In Framework (Issue May). http://people.dsv.su.se/~bjorck/files/thesis-book.pdf

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. Proceedings New Security Paradigms Workshop, 97–104. https://doi.org/10.1145/508185.508187

Blackwell, C. (2009). A security architecture to protect against the insider threat from damage, fraud and theft. Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies - CSIIRW 09. doi:10.1145/1558607.1558659.

Bosch, S. van den. (2014). Designing Secure Enterprise Architectures. Enschede. https://doi.org/10.1002/chem.200903310.

Braa, Hanseth, Heywood, Mohammed, & Shaw. (2007). Developing Health Information Systems in Developing Countries: The Flexible Standards Strategy. MIS Quarterly, 31(2), 381. doi:10.2307/25148796.

Briney A. (2001). Information security industry survey. Available from: http://www.infosecuritymag.com.

Brunton, G., Stansfield, C., & Thomas, J. (2012). Finding relevant studies. In: D. Gough, S.

Brunton, J., & Thomas, J. (2012). Information management in reviews. In: D. Gough, S. Oliver, & J. Thomas (Eds.), An introduction to systematic reviews (pp. 83–106). London: Sage Publications Ltd.

Bulgurcu, Cavusoglu, & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523. doi:10.2307/25750690

Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organizations Enterprise Architecture through SABSA®. Information Security Journal: A Global Perspective, 21(1), 47-54. doi:10.1080/19393555.2011.629341.

Brink, E., Dellve, L., Hallberg, U., Abrahamsson, K. H., Klingberg, G., & Wentz, K. (2006). Constructing grounded theory. A practical guide through qualitative analysis. International Journal of Qualitative Studies on Health and Well-Being, 1(3). https://doi.org/10.3402/qhw.v1i3.4932.

Çağdaş, V., & Stubkjær, E. (2011). Design research for cadastral systems. Computers, Environment and Urban Systems, 35(1), 77-87. doi: 10.1016/j.compenvurbsys.2010.07.003.

Cardno, C. A. (2019). Financial Services Technology 2020 and Beyond. Civil Engineering

Magazine Archive, 89(1), 70–83. https://doi.org/10.1061/ciegag.0001345.

Chakrabarti, A. (2010). A course for teaching design research methodology. Artificial Intelligence for Engineering Design, Analysis and Manufacturing, 24(3), 317-334. doi:10.1017/s0890060410000223.

Chang, A. J., & Yeh, Q. (2006). On security preparations against possible IS threats across industries. Information Management & Computer Security, 14(4), 343-360. doi:10.1108/09685220610690817.

Charmaz, K. (2006). Constructing Grounded Theory: A Practical Guide through Qualitative Analysis, London: SAGE Publications, Inc.

Chaudhry, P. E., Chaudhry, S. S., Clark, K. D., & Jones, D. S. (2013). Enterprise Information Systems Security: A Case Study in the Banking Sector. Lecture Notes in Business Information Processing Enterprise Information Systems of the Future, 206-214. doi:10.1007/978-3-642-36611-6_18.

chneider, E. A. (2000). Security architecture-based system design. Proceedings of the 1999 Workshop on New Security Paradigms - NSPW 99. doi:10.1145/335169.335185.

Christopher Peake (2003). Red Teaming: The Art of Ethical Hacking- SANS Institute Information Security Reading Room.

Cole, R., Purao, S., Rossi, M., & Sein, M. K. (2005). Running Head : PROACTIVE RESEARCH APPROACHES Being Proactive : Where Action Research meets Design Research. Running Head: PROACTIVE RESEARCH APPROACHES., 1–21.

Contreni, J. J. (1980). Ruy Afonso da Costa Nunes, History of Education in the Middle Ages. São Paulo: Editora Pedagógica e Universitária Ltda., 1979. Paper. Pp. ix, 313; 1 map. Speculum, 55 (03), 630. doi: 10.1017 / s0038713400158853.

C. Kothari (2004), Research Methodology: Methods and Techniques, India: New Age International (R) Ltd.

Coetzee, M. (2012). Towards a Holistic Information Security Governance Framework for SOA. 2012 Seventh International Conference on Availability, Reliability and Security. doi:10.1109/ares.2012.62

Comer, D. (2017). Essentials of Computer Architecture. Essentials of Computer Architecture. https://doi.org/10.1201/9781315226262.

Computer Security – ESORICS 2006. (2006). Lecture Notes in Computer Science. doi:10.1007/11863908.

CSA.(2012). SecaaS Category 10 Network Security Implementation Guidance. Secaas Implementation Guidance, September.

Cziner, K., Mutafungwa, E., Lucenius, J., & Järvinen, R. (2007). Critical Information Infrastructure Protection in the Baltic Sea Area: The Case …. http://www.helsinki.fi/aleksanteri/civpro/publications/WP6.pdf

Daniel Gebrehawariat (2017). Assessment of the Effectiveness of Card Banking Security in Ethiopian Financial Sector, School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia.

David Garlan and Mary Shaw (1993). An introduction to software architecture. In Advances in Software Engineering and Knowledge Engineering, edited by V. Ambriola and G. Tortora, World Scientific Publishing Company.

[Defense Information Systems Agency, Center for Standards (1996). Department of Defense (DoD) Goal Security Architecture (DGSA), Version 3.0. Volume 6 of Department of Defense Technical Architecture Framework for Information Management (TAFIM).

DeLooze (2020). Applying security to an enterprise using the Zachman Framework, SANS.

Deloitte Touche Tohmatsu. (2006). 2006 Global Security Survey. Security, 1–44.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314. doi:10.1111/j.1365-2575.2006.00219. x.

Dontamsetti, M., & Narayanan, A. (2009). Impact of the human element on information security. In Social and Human Elements of Information Security: Emerging Trends and Countermeasures. https://doi.org/10.4018/978-1-60566-036-3.ch003.

Doughty, K. (2003). Implementing enterprise security: A case study. Computers & Security, 22(2), 99-114. doi:10.1016/s0167-4048(03)00205-0.

D. Myers (2009). Qualitative Research in Business & Management. London: Sage 2009. Qualitative Research in Accounting & Management, 6(4), 292-296. doi:10.1108/11766090910989536.

Dresch, A., Lacerda, D. P., & Valle, A. J. (2015). Design Science Research a Method for Science and Technology Advancement. Cham: Springer International Publishing.

Dutta, A., & Mccrohan, K. (2002). Managements Role in Information Security in a Cyber Economy. California Management Review, 45(1), 67-87. doi:10.2307/41166154 .

Edward A. Schneider, Edward A. Feustel, and Ronald S. Ross (1997). Assessing DoD Goal Security Architecture (DGSA) Support in Commercially Available Operating Systems and Hardware Platforms. IDA Paper P-3375.

Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach (1997). Web Spoofing: An Internet Con Game- Technical Report 540–96.

Eekels, J., & Roozenburg, N. (1991). A methodological comparison of the structures of scientific research and engineering design: Their similarities and differences. Design Studies, 12(4), 197-203. doi:10.1016/0142-694x (91)90031-q.

Eloff, J. H. P., & Eloff, M. (2003). Information security management: a new paradigm. Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology, 130–136. http://dl.acm.org/citation.cfm?id=954014.954028.

Ekstedt, M., & Sommestad, T. (2009). Enterprise architecture models for cyber security analysis. 2009 IEEE/PES Power Systems Conference and Exposition. doi:10.1109/psce.2009.4840267.

EPPI Centre (2013). http://eppi.ioe.ac.uk/cms/.

Fàbregues, S., & Paré, M. (2007). Charmaz, Kathy C. (2006). Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis. Papers. Revista De Sociologia, 86, 284. doi:10.5565/rev/papers/v86n0.825.

FDRE. (2006). The national information and communication technology.

FDRE. (2009). The national information and communication technology policy and strategy.

Federal Democratic of Ethiopia (2006). Federal Negarit Gazeta, information Network Security Agency Establishment Council of Ministers Regulation No.130/2006,13thYear No. 5 Addis Ababa24th November, 2006, Ethiopia.

Federal Democratic of Ethiopia Information Network Technology Agency (2016) Critical Mass Cyber Security Requirement Standard Version 1.0.

Federal Democratic of Ethiopia (2012). Federal Negarit Gazeta, Telecom Fraud Offence Proclamation No. 761/2012,18thYear No. 61 Addis Ababa 4thSeptember, 2012, Ethiopia.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management and Computer Security, 22(5), 410– 430. https://doi.org/10.1108/IMCS-07-2013-0053

Feustel, E. A., & Mayfield, T. (1998). The DGSA: Unmet information security challenges for operating system designers. ACM SIGOPS Operating Systems Review, 32(1), 3-22. doi:10.1145/280559.280562.

Fischhoff, B. (2002). Assessing and communicating the risks of terrorism. In A.H. Teich, S.D.

Furnell, S., & Clarke, N. (2005). Organizational security culture: Embedding security awareness, education, and training. Proceedings of the 4th World Conference on Information Security Education, 11(Dti), 67–74.

G. Gopalakrishna (2011) Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds‖, RBI, Mumbai, Maharashtra. https://www.bankinfosecurity.asia/rbis-guidelines-overview-a-4045.

Gibbons, A. S., & Bunderson, C. V. (2005). Explore, Explain, Design. Encyclopedia of Social Measurement, 927-938. doi:10.1016/b0-12-369398-5/00017-7.

Gough, D., Oliver, S., & Thomas, J. (2012). An introduction to systematic reviews. London: Sage Publications Ltd.

Greenwald, Steven J. (1996). "A New Security Policy for Distributed Resource Management and Access Control." Proceedings of the 1996 Workshop on New Security Paradigms - NSPW 96, doi:10.1145/304851.304870.

Hailu, H. (2015). The State of Cybercrime Governance in Ethiopia. 1–35.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377-397. doi:10.1108/09685220810908796.

Hair, Joseph F. , Black, Jr, William C. Babin, Barry J. & Anderson, R. E. (2014). Pearson - Multivariate Data Analysis, 7/E - Joseph F. Hair, Jr, William C. Black, Barry J. Babin & Rolph E. Anderson. Pearson New International Edition, 816.

Hammerstrom, K., Wade, A., & Jorgensen, A.-M. K. (2010). Searching for studies: A guide to information retrieval for Campbell Systematic Reviews (Vol. 1). Oslo: The Campbell Collaboration.

Harold F. Tipton, Micki Krause (2007). "Information Security Management Handbook: Information Security Governane". Auerbach Publications, USA. 6thed.

Hamill, J., Deckro, R. F., & Kloeber, J. M. (2005). Evaluating information assurance strategies. Decision Support Systems, 39(3), 463-484. doi: 10.1016/j.dss.2003.11.004.

Heaney, J., Hybertson, D., Reedy, A., Chapin, S., Bollinger, T., Williams, D., & Kirwan, M. (2002). Information Assurance for Enterprise Engineering. MITRE Report, August, 1–20.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly: Management Information Systems, 28(1), 75–105. https://doi.org/10.2307/25148625.

H. G. Goldman. (2010). Building Secure, Resilient Architectures for Cyber Mission Assurance.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125. doi:10.1057/ejis.2009.6.

Hutchinson, D., & Warren, M. (2003). Security for Internet banking: A framework. Logistics Information Management, 16(1), 64-73. doi:10.1108/09576050310453750.

IBM (2008). Take a holistic approach to business-driven security.
IEEE International Conference on Services Computing (SCC 2008). (2007). Computer, 40(12), C3-C3. doi:10.1109/mc.2007.430.

INSA (2020). cyber-attack statistics. Available https://www.insa.gov.et/web/guest/-/-113.

INSA (2019). Security threats. Available at https://www.insa.gov.et/de/web/en/information-security

International Telecommunication Union. (2017). Global Cybersecurity Index (GCI) 2017. In ITU-D Global. https://doi.org/10.1111/j.1745-4514.2008.00161.x.

ISO/IEC 27001(2009). "Information technology – Security techniques – Information security management systems – Overview and Vocabulary". Available https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Jing Liu, Yang Xiao, Hui Chen, Suat Ozdemir, Srinivas Dodle and Vikas Singh (2010). A Survey of Payment Card Industry Data Security Standard, pp.287-303.

Johnson, T., Acedo, C., Kobourov, S., & Nusrat, S. (2015). Analyzing the Evolution of the Internet. Eurographics Conference on Visualization (EuroVis).

Johansson, E. (2005). Assessment of Enterprise Information Security–How to make it Credible and efficient. Information Security, October. http://en.scientificcommons.org/7645483.

John W. Creswell (2013). Research Design Qualitative, Quantitative, and Mixed Methods Approaches. 4th edn. SAGE Publications, Inc.

Johansson, E., & Johnson, P. (2005). Assessment of enterprise information security-an architecture theory diagram definition. Proc. of CSER, 136–146. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.2922&rep=rep1&type=pdf

Johannesson, P., & Perjons, E. (2014). Introduction. An Introduction to Design Science, 1-19. doi:10.1007/978-3-319-10632-8_1.

Joseph Migga Kizza (2009). Computer Communications and Networks : A Guide to Computer Network Security book.

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert Scale: Explored and Explained. British Journal of Applied Science & Technology, 7(4), 396-403. doi:10.9734/bjast/2015/14975.

Junior, A. E., & Santos, E. M. (2015). Adoption of Information Security Measures in Public Research Institutes. Proceedings of the 12th CONTECSI International Conference on Information Systems and Technology Management. doi:10.5748/9788599693117-12contecsi/ps-3155.

Kadam, W. (2007). Information Security Policy Development and Implementation. Information Systems Security,16(5), 246-256. doi:10.1080/10658980701744861.

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2007). Senior Executives Commitment to Information Security – from Motivation to Responsibility. Computational Intelligence and Security Lecture Notes in Computer Science, 833-838. doi:10.1007/978-3-540-74377-4_87.

Kankanhalli, A., Teo, H., Tan, B. C., & Wei, K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139-154. doi:10.1016/s0268-4012(02)00105-6.

Kappelman, L., McLean, E., Luftman, J., & Johnson, V. (2013). Key issues of IT organizations and their leadership: The 2013 SIM IT trends study. MIS Quarterly Executive, 12(4), 227– 240.

Kark, K., Stamp, P., Penn, J., Koetzle, L., & Mulligan, J. A. (2007). Defining A High-Level Security Framework. Putting Basic Security Principles to Work. Avaible:https://www.forrester.com/report/Defining+A+HighLevel+Security+Framework/-/E-RES40996#

Kaur, A. (2015). How is Digital Infrastructure Adopted and Assimilated ? The IPv6 Story Awinder Kaur A thesis submitted to Auckland University of Technology in fulfillment of the requirements for the degree of Doctor of Philosophy (PhD) Faculty of Business and Law Depar.

Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger & Samir Chatterjee (2007) A Design Science Research Methodology for Information Systems Research, Journal of Management Information Systems, 24:3, 45-77, DOI: 10.2753/MIS0742-1222240302.

Khan, M., & Barua, S. (2009). The status and threats of information security in the banking sector of Bangladesh: Policies required. Bangladesh Journal of MIS, January. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1569207.

Khochare, N., & Meshram, B. B. (2012). Tool to Detect and Prevent Web Attacks. International Journal of Advanced Research in Computer Engineering, 1(4), 375–378.

Killmeyer, J. (2006). Information Security Arhictecture. In Pediatrics: Vol. 134 Suppl. https://doi.org/10.1542/peds.2014-134S2.

Kim, S., & Leem, C. S. (2004). An information engineering methodology for the security strategy planning (pp. 597--607): Springer.

Kim, S., & Leem, C. S. (2004). An Information Engineering Methodology for the Security Strategy Planning. Computational Science and Its Applications – ICCSA 2004 Lecture Notes in Computer Science, 597-607. doi:10.1007/978-3-540-24707-4_71.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management & Computer Security, 22(1), 115-126. doi:10.1108/imcs-01-2013-0005.

Kim, S., & Leem, C. S. (2005). Enterprise security architecture in business convergence environments. Industrial Management & Data Systems, 105(7), 919-936. doi:10.1108/02635570510616111.

Kinser, P., (2007). Enterprise Security Architecture, Information System Security Association, [online] Available at: http://www.issa-centralva.org/

Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering-A tertiary study. Information and Software Technology, 52(8), 792–805. https://doi.org/10.1016/j.infsof.2010.03.006.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28(7), 493-508. doi: 10.1016/j.cose.2009.07.001.

Korhonen, J. J., Yildiz, M., & Mykkänen, J. (2009). Governance of Information Security Elements in Service-Oriented Enterprise Architecture. 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks. doi:10.1109/i-span.2009.158.

K. Peffers, T. Tuunanen, C. E. Gengler, M. Rossi, W. Hui, V. Virtanen And J. Bragge (2006), "The Design Science Research Process: A Model for Producing and Presenting Information Systems Research".

KragBrotby W. (2009). "Information Security Governance: Guidance for Information Security Managers" IT Governance Institute (ITGI). USA. Availabe at: https://www.isaca.org.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289-296. doi:10.1016/j.cose.2006.02.008.

Krohn, M. D., & Massey, J. L. (1980). Social Control and Delinquent Behavior: An Examination of the Elements of the Social Bond. The Sociological Quarterly, 21(4), 529-544. doi:10.1111/j.1533-8525.1980.tb00634.x

Kuechler B., Vaishnavi V. (2011) Extending Prior Research with Design Science Research: Two Patterns for DSRIS Project Generation. In: Jain H., Sinha A.P., Vitharana P. (eds) Service-Oriented Perspectives in Design Science Research. DESRIST 2011. Lecture Notes in Computer Science, vol 6629. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20633-7_12.

Kugley S, Wade A, Thomas J, Mahood Q, Jørgensen AMK, Hammerstrøm K, Sathe N. (2016) Searching for studies: A guide to information retrieval for Campbell Systematic Reviews. Campbell Methods Guides:1 DOI: 10.4073/cmg.2016.1.

Lee, S. M., Lee, S., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718. doi:10.1016/j.im.2003.08.008.
Le Moigne, J. -L. (1994). Le constructivisme tome 1: Fondements. Paris: ESF Editeur.

Lemma Lessa and Abiy Woretaw, (2012). Information security culture in the banking sector in Ethiopia.

L.F. Kwok, D. Longley (1999), Information security management and modeling, Information Management & Computer Security, pp.30–39.

Lindstrom, P. (2004). Intrusion Prevention Systems (Ips): Next Generation Firewalls. March. www.spiresecurity.com.

Liu, D., Wang, X., & Camp, L. J. (2009). Mitigating Inadvertent Insider Threats with Incentives. Financial Cryptography and Data Security Lecture Notes in Computer Science, 1-16. doi:10.1007/978-3-642-03549-4_1.

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., & Singh, V. (2010). A survey of payment card industry data security standard. IEEE Communications Surveys and Tutorials, 12(3), 287–303. https://doi.org/10.1109/SURV.2010.031810.00083.

Lowman, T. and Mosier, D (1997). Applying the DoD goal security architecture as a methodology for the development of system and enterprise security architectures. Computer Security Applications Conference, pp.183-193.

Luker, M. and Petersen, R. (2003). Computer and Network Security in Higher Education, EDUCAUSE, [online] Available at :<http://net.educause.edu/ir/library/pdf/pub7008j.pdf>.

Lallie, H. S. (2010). A Simple Enterprise Security Architecture (SESA): Towards a Pedagogic Architecture for Teaching Cyber Security. 1–14.

Lee, S. M., Lee, S., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718. doi:10.1016/j.im.2003.08.008.

Maki, P. L. (2002). Developing an . Journal of Academic Librarianship, 16(1/2), 8.

Maiwald, E., Osborne, M., & Brownlow, J. (2002). Security Planning & Disaster Recovery Acquisitions Editor.

Manson, N. (2006). Is operations research really research? ORiON, 22(2). doi:10.5784/22-2-40.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision Support Systems, 15, 251–266.

Mark R. Ousley, (2013). "Complete Reference: Information Security". 2nd edition, McGraw, USA.

Martins, A., & Elofe, J. (2002). Information Security Culture. IFIP Advances in Information and Communication Technology Security in the Information Society, 203-214. doi:10.1007/978-0-387-35586-3_16.

Merkow, M. S., & Breithaupt, J. (2014). Information Security: Principles and Practices Second Edition Warning and Disclaimer. In Library of Congress Control Number.

McIlwraith, A. (2006). Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness. 169. http://books.google.com/books?hl=en&lr=&id=XnBOhKHJKMQC&pgis=1.

Mengistu Bogale Ayele (2016). Auditing IT and IT Governance in Ethiopia, School of Information Science, Addis Ababa University, and Addis Ababa, Ethiopia.

Mentzer, J. T., & Flint, D. J. (1997). Validity in logistics research. Journal of Business Logistics, 18(I), 199–217.

Michael N., Kelley D., Victoria Y. (2017). An introduction to information security evaluation. Journal of Information Processing and Management, 48(6), 320–332. https://doi.org/10.1241/johokanri.48.320.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 36(1), 42-57. doi: 10.1016/j.jnca.2012.05.003.

Mohammed M., Alexander A. (2017). Information Security in an Organization. International Journal of Computer (IJC), 4523, 100–116. http://ijcjournal.org/.

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. Journal of Economic Perspectives, 23(3), 3-20. doi:10.1257/jep.23.3.3.

Morrill, M. (2007). Information Security as a People Problem. http://it.toolbox.com/blogs/managing-infosec/information-security-as-a-peopleproblem-13777.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18(2), 126-139. doi:10.1057/ejis.2009.10.

Nickolov, E. (2005). Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations. Information & Security, 17, 105–119. http://www.comw.org/tct/fulltext/05nickolov.pdf

NIST(1998). Information Technology Security Training Requirements : A Role- and Performance-Based Model Form SF298.

Nelson, & S.J. Lita (2003), Science and technology in a vulnerable world (pp. 51-64). Washington, DC: Supplement to AAAS Science and Technology Policy Yearbook 2003.

Oda, S. Michelle, Huirong Fu, and Ye Zhu (2009). "Enterprise information security architecture a review of frameworks, methodology, and case studies." Computer Science and Information Technology, 2009. ICCSIT 2009. DOI: 10.1109/ICCSIT15763.2009

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, DESRIST '09, June 2014. https://doi.org/10.1145/1555619.1555629.

Office of CIO of Ministry of Citizen's services in British Columbia (2010). Information Security Architecture. Available at: http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/summaries/25_info_security_architecture.pdf.

Olawsky, D., Fine, T., Schneider, E., & Spencer, R. (1996). Developing and using a "policy neutral" access control policy. Proceedings New Security Paradigms Workshop, Part F1294, 60– 67. https://doi.org/10.1145/304851.304866.

Ole Hanseth (2002). From systems and tools to networks and infrastructures - from design to cultivation. Towards a theory of ICT solutions and its design methodology implications.

Oliver, & J. Thomas (2007). An introduction to systematic reviews. London: Sage Publications Ltd.

Oost, D., & Chew, E. (2012). Investigating the concept of information security culture. Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions, December, 1–12. https://doi.org/10.4018/978-1-4666-0197-0.ch001.

OSA (2020). defines the security architecture. [online] Available at: https://www.opensecurityarchitecture.org/cms/definitions.

Oxford University Press. Oxford Dictionaries. Available: http://oxforddictionaries.com. <accessed 01/02/2020 >

Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security : Individual , Culture and Security Environment. Science And Technology, DSTO-TR-2484, 45. https://doi.org/10.14722/ndss.2014.23268.

Pauline Rogito (2017). Multi-tiered security architecture for information infrastructure protection in selected commercial banks in Kenya.

Pavlovski, C. (2013). A Multi-Channel System Architecture for Banking. International Journal

of Computer Science, Engineering and Applications, 3(5), 1–12. https://doi.org/10.5121/ijcsea.2013.3501.

Peter Gutman (2003). Cryptographic Security Architecture: Design and Verification.

Pfleeger, C. P., S. L. Pfleeger (2003). Security in Computing. Upper Saddle River, New Jersey, Prentice Hall.

Preez, D. W., & Pieterse, V. (2006). Calculating Compliance Standards. Issa, 1–11. https://doi.org/10.3354/dao02845.

Porter, M. and Millar, V., (1985). How information gives you competitive advantage, Harvard Business Review. Available at :< https://www.gospi.fr/IMG/pdf/how_information_ gives you_ competitive advantage-porter-hbr-1985.pdf >

Pries-Heje, & Baskerville. (2008). The Design Theory Nexus. MIS Quarterly, 32(4), 731. doi:10.2307/25148870.

Procaccianti, G., & Routsis, A. (2016). Energy Efficiency and Power Measurements: An Industrial Survey. Proceedings of ICT for Sustainability 2016. doi:10.2991/ict4s-16.2016.9. Peterson, G. (2007). Security Architecture Blueprint. Business, 1–12. https://doi.org/10.1007/s11859-006-0126-x.

Rachamadugu, V., & Anderson, J. A. (2008). Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure. 2008 IEEE International Conference on Services Computing. doi:10.1109/scc.2008.46.

Ramadan, A. B., & Hefnawi, M. (2007). A Network Security Architecture Using The Zachman Framework. Managing Critical Infrastructure Risks NATO Science for Peace and Security Series C: Environmental Security, 133-143. doi:10.1007/978-1-4020-6385-5_8.

Reba, B. B. (2005). Etiopian Telecommunications Agency State of Cyber Security in Ethiopia. June.

Robert K. Yin. (2014). Case study research design and methods (5th ed.). Thousand Oaks, CA: Sage.

Romme, A. G. (2003). Making a Difference: Organization as Design. Organization Science, 14(5), 558-573. doi:10.1287/orsc.14.5.558.16769.

Royds J. (2009). Virtual battlefield. CIR Magazine; August.

Ruighaver, A.B., Maynard, S.B. & Chang (2007). Organizational security culture: Extending the end-user perspective. Computers and Security, 26, 56-62.

SABSA (2008). The SABSA Method. [online] Available at: <http://www.sabsa.org/the-sabsamethod.aspx>.

Sangani, N. K., Vithani, T., & Madiajagan, M. (2013). Advantages of components in security & privacy architecture as a service for small and medium enterprises. Lecture Notes in Engineering and Computer Science, 2 LNECS, 1226–1229.

SANS (2002). "A Preparation Guide to Information Security Policy". SANS Institute.

Sandy Bacik (2011). Federal Networking and Information Technology Research and Development (NITRD) Program Tailored Trustworthy Spaces : Solutions for the Smart Grid Arlington , VA Workshop Report.

Sarah Pramanik & Northrop Grumman (2013). Security Architecture Approaches, Real-Time Information Assurance.

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: Increased trust by an appropriate information security culture. 14th International Workshop on Database and Expert Systems Applications. Proceedings. doi:10.1109/dexa.2003.1232055.

Scholtz, T., Byrnes, C. and Heiser, J. (2005). Establish an Effective Information Security Program, Part 1: Structure and Content, Gartner, [online] Available at: http://www.gartner.com/DisplayDocument?ref=g_search&id=485572.

Schneier, B. (2000). Secrets and lies: digital security in a networked world [Books]. IEEE Spectrum, 37(10), 15–16. https://doi.org/10.1109/mspec.2000.873914.

Schuldt, H. (2008). Multi-tier Architecture. Encyclopedia of Database Systems, 1–3. https://doi.org/10.1007/978-1-4899-7993-3_652-2.

Shiozaki, T., Okuhara, M., & Yoshikawa, N. (2007). Fujitsu enterprise security architecture. Fujitsu Scientific and Technical Journal, 43(2), 153–158.

Solms, R. V. (1999). Information security management: Why standards are important. Information Management & Computer Security, 7(1), 50-58. doi:10.1108/09685229910255223.

Scholtz, T. (2008). The Structure and Content of an Information Security Architecture Framework, Gartner, [online] Available at (Restricted to the members): <http://www.gartner.com/DisplayDocument?id=686311> [Accessed 21 April 2020].

Seuring, S., & Gold, S. (2012). Conducting content-analysis based literature reviews in supply chain management. Supply Chain Management, 17(5), 544–555. https://doi.org/10.1108/13598541211258609.

Shahram J. &Farzaneh F. (2011). Enterprise Architecture & Security Architecture Development, Department of Informatics, Lund University.

Sherwood, John. Clark; Andrew; Lynas, David (2003). "Systems and Business Security Architecture." SABSA Limited.

Sherwood, J., Clark, A., & Lynas, D. (2005). Enterprise security architecture: a business-driven approach: Backbeat Books.

Sherwood, J., Clark, A., & Lynas, D. (2009). Enterprise security architecture. Information Security Management Handbook, Sixth Edition, 2491–2502. https://doi.org/10.1201/9781439833032.ch188.

Sherwood, J. et al (n.d). Sherwood Applied Business Security Architecture. [WWW] SABSA Institute. Available from: http://www.sabsa.org. [Accessed 19/02/2020].

Silowash, George, et al. (2012) "Common Sense Guide to Mitigating Insider Threats 4th Edition." doi:10.21236/ada585500.

Shirey, R. (2000) "Internet Security Glossary." doi:10.17487/rfc2828.

Siponen M., Pahnila S., and Mahmood A., (2007). "Employees' Adherence to Information Security Policies: An Empirical Study." New Approaches for Security, Privacy and Trust in Complex Environments IFIP International Federation for Information Processing, pp. 133–144., doi:10.1007/978-0-387-72367-9_12.

Simon, H. A. (1996). The sciences of the artificial (3rd ed.). USA: MIT Press.

Simeneh T. (2013). Prospects and challenges of private commercial banks in Ethiopia.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41. doi:10.1108/09685220010371394.

S.M. Furnell, M. Gennatou and P.S. Dowland (2002). A prototype tool for information security awareness and training.

S.M. Furnell, M. Gennatou and P.S. Dowland (2002). "A Prototype Tool for Information Security Awareness and Training." Logistics Information Management, vol. 15, no. 5/6, pp. 352– 357., doi:10.1108/09576050210447037.

Solms, R. V., & Solms, S. (. (2006). Information Security Governance: A model based on the Direct–Control Cycle. Computers & Security, 25(6), 408-412. doi: 10.1016/j.cose.2006.07.005.

Son, J. (2011). Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to follow IS Security Policies. Information and Management 48, 296–30. https://doi.org/10.1016/j.im.2011.07.002.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). "Analysis of End User Security Behaviors." Computers & Security, vol. 24, no. 2, 2005, pp. 124–133., doi: 10.1016/j.cose.2004.07.001.

Smith, Stephen, and Rodger Jamieson (2006). "Determining Key Factors in E-Government Information System Security." Information Systems Management, vol. 23, no. 2, 2006, pp. 23– 32., doi:10.1201/1078.10580530/45925.23.2.20060301/92671.4.

Shinder, T. W., & Shinder, D. L. (2005). Evolution of a Firewall: From Proxy 1.0 to ISA 2004. Dr. Tom Shinders Configuring ISA Server 2004, 1-77. doi:10.1016/b978-193183619-7/50008-3.

Singh, A., Vaish, A., & Keserwani, P. K. (2014). Information Security: Components and Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 4(1), 2277–128.

Stoneburner, Gary (2001). "Underlying Technical Models for Information Technology Security" doi:10.6028/nist.sp.800-33.

Sun, J., & Chen, Y. (2008). Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture. 2008 International Seminar on Future Information Technology and Management Engineering. doi:10.1109/fitme.2008.30.

Steven J. Greenwald (1996). A new security policy for distributed resource management and access control. In Proceedings of the New Security Paradigms Workshop, pages 74-86, Lake Arrowhead, CA.

Stoneburner, G. (2001). Underlying technical models for information technology security: doi:10.6028/nist.sp.800-33.

Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. Information Systems Management, 23(2), 23-32. doi:10.1201/1078.10580530/45925.23.2.20060301/92671.4.

Singh Brar, T. P., Sharma, D., & Singh Khurmi, S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research.

Tahajod, M., Iranmehr, A., Iranmehr, A., & Darajeh, M. (2009). A roadmap to develop enterprise security architecture. 2009 International Conference for Internet Technology and Secured Transactions, (ICITST). doi:10.1109/icitst.2009.5402639.

Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawa, H. (1990). Modeling design processes.

AI Magazine, 11(4), 37–48.

Talabis & Martin, J. (2012). Information Security Risk Assessment: Data Analysis. Information Security Risk Assessments, 105-146. doi:10.1016/b978-1-59-749735-0.00004-x.

Tariku Adane (2011). Mining Insurance Data Fraud Detection: The case of African Insurance Share Company, School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia.

Thomson, M., & Solms, R. V. (1998). Information security awareness: Educating your users effectively. Information Management & Computer Security, 6(4), 167-173. doi:10.1108/09685229810227649.

Thomson, K., Solms, R. V., & Louw, L. (2006). Cultivating an organizational information security culture. Computer Fraud & Security, 2006(10), 7-11. doi:10.1016/s1361-3723(06)70430-4.

Tisn. (2007). Secure Your Information : Information Security Principles for Enterprise Architecture. Security, June.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence informed management knowledge by means of systematic review. Journal of International Management, 19(4), 390–406. https://doi.org/10.1016/j.intman.2013.03.011.

Technology and Management Engineering (2008). FITME '08: Proceedings of the 2008 International Seminar on Future Information Technology and Management Engineering.

Tom Lowrnan and Douglas Mosier (1997). Applying the DoD Goal Security Architecture as a methodology for the development of system and enterprise security architectures, lnProeeedings of the Thirteenth Annual Computer Security Applications Conference, pages 183-193, San Diego, CA, IEEE Computer Society.

Terry Chia (2012), Confidentiality, Integrity, Availability: The three components of the CIA Triad. Available at: https://www.coursehero.com/file/28625952/Confidentiality-Integrity-Availability-The-three-components-of-the-CIA-Triad-Stack-Exchange-Sec/.

Tilahun Muluneh Arage (2017). A study of Employees' Information Security Policy Violation and Rational Choice Theory: The Case of Ethiopia, School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia.

Thorn, A., Christen, T., Gruber, B., Portman, R. and Ruf, L., (2008). What is a Security Architecture? Information Security Society Switzerland, [online] Available at: < https://polimetlase.wordpress.com/2014/03/04/what-is-security-architecture/> [Accessed 18 April 2020].

Tracy, R. P. (2007). IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards. Information Systems Security, 16(2), 114-122. doi:10.1080/10658980601051706.

Union, I. T. (1991). International Telecommunication Union (ITU). 987–990. Security architecture for Open Systems Interconnection for CCITT applications. ITU-T Recommendation X.800. https://doi.org/10.18356/cbabbce2-en.

Veiga, A. D., & Eloff, J. H. (2007). An Information Security Governance Framework. Information Systems Management, 24(4), 361-372. doi:10.1080/10580530701586136.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? Computers and Security, 24(2), 99–104. https://doi.org/10.1016/j.cose.2005.02.002.

Vaishnavi , V . K . and W . Kuechler (2015). Design Science Research Methods and Patterns : Innovating Information and Communication Technology 2nd ed . New York , CRC Press ... June.

Vaishnavi, V., Kuechler, W., and Petter, S. (Eds.) (2004/19). "Design Science Research in Information Systems" January 20, 2004 (created in 2004 and updated until 2015 by Vaishnavi, V. and Kuechler, W.); last updated (by Vaishnavi, V. and Petter, S.), June 30, 2019. URL: http://www.desrist.org/design-research-in-information-systems/.

Van Aken, J. E. (2005). Management research as a design science: Articulating the research products of mode 2 knowledge production in management. British Journal of Management, 16(1), 19–36. https://doi.org/10.1111/j.1467-8551.2005.00437.x

Vroom, C., & Solms, R. V. (2004). Towards information security behavioral compliance. Computers & Security, 23(3), 191-198. doi: 10.1016/j.cose.2004.01.012.

Walters, L. M. (2007). A draft of an information systems security and control course. Journal of Information Systems, 21 (1), 123-148. Availabe at: https://doi.org/10.2308/jis.2007.21.1.123.

Walls, J. G., Widmeyer, G. R., & Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. Information Systems Research, 3(1), 36-59. doi:10.1287/isre.3.1.36.

Warren P. (2008). Tactical Perimeter Defense book: Becoming A Security Network Specialist, Page 48-49.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. Learning, 269, 289.

Whitman, M. E. (2003). Enemy at the gate. Communications of the ACM, 46(8), 91-95. doi:10.1145/859670.859675.

Yoo, C., Kang, B. T., & Kim, H. K. (2015). Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimedia Tools and Applications, 74(10), 3289–3303. https://doi.org/10.1007/s11042-014-1888-3.

Zuccato, A., (2002). Towards a systemic holistic security management. M.Sc. Karlstad University.

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

Addis Ababa University
College of Natural Science
School of Information Science

Date: March 11, 2020
Ref No. SIS/61/2020/2012

To:- National Bank of Ethiopia
Addis Ababa

Subject:- Student Chamo Gezahegn

Dear Sir /Madam,

Student Chamo Gezahegn (ID.No GSE/2977/10) is graduate student at the School of Information System, Addis Ababa University. He is currently conducting a MSc. Thesis research under the title "Develop multi tiered Security Architecture for Information infrastructure for Ethiopia Banking Industry".

I would like to thank you in advanced for all the assistance that you would provide to the student.

With Regards

Tibebe Beshah (PhD)
Head, School of Information Science

✉: 1176 Email: information_cci_cns@aau.edu.et ☎: +251-(11)-122-91-91

Appendix A: User Questionnaire

Dear Participant,

I'm currently conducting a research which entitled "Multi-tiered Security architecture towards Information Infrastructure protection" assumed as partial fulfillment of the requirements for the Degree of Master of Science in Information Systems at Addis Ababa University. The objective of this study is to Develop Multi-tiered Security architecture towards Information Infrastructure protection based on the current practice of information security. NBE has approved our request and gives us the "go-ahead" permission to distribute questionnaire and collect data from selected samples of the bank. The data collected from cooperative respondents will help our esteemed bank to realize the information security enhancement and to protect financial institutions from any security attacks.

All the data you provide will be kept confidential and will be used for academic purpose only. We would like greatly appreciate your cooperation and taking time to complete our questionnaire.

Thank you for your kind cooperation and participation in this research!

Chamo Gezahegn,

Phone: +251910622115

Instructions!

Please don't write your name.

Please put thick mark √ on the appropriate box/place which shows your choice along each statement.

Part 1: Demographic Data

1. Gender

A. Male ☐ B. Female ☐

2. Education Status

A. Diploma ☐ B. Bachelor Degree ☐ C. Master's Degree ☐ D. Ph. D. ☐

3. Work Experience

A. 5 years or less ☐ B. 6-10 years ☐ C. 11-15 years ☐ D. 15 years or above ☐

Part 2 = Questions on Security Assessments for National Bank of Ethiopia.

Likert scale numbers, range from 1-5, denote the following weights.

1= Strongly Disagree 2= Disagree 3= Neutral 4= Agree 5= Strongly Agree

No	Security Assessments Questions	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	All systems are up to date with patches					
2	All needed ports are open					
3	All needed services are open					
4	Firewall Rule are set analysis					

5	All network devices are positioned properly and correctly					
6	All secure and non-secure interfaces are identified					
7	History of the All device is recorded					
8	Device Logs are checked regularly and there is a responsible body for creating and deleting accounts					
9	There is responsible body for reviewing Logs					
10	There is a process of change management					
	VPN and Proxy related Questions					
1	The Configurations of Cisco security profiles are used by users to access the network					
2	Your bank has VPN and distribution implementation policy					
3	Your bank has VPN access and controls need to be on every PC					
4	Your bank has internet policy					
	Http traffic being scanned for antivirus					

Strongly ... Agree Strongly

5	**Your banks proxy has a good way to stop spam**					
	Switch and Router related questions:					
1	**Your organization network connection is positioned properly.**					
2	**All switches and routers are configured properly and a good authentication method are used.**					
3	**All polices are configured and users are authorized properly**					
4	**All Devices Obtain an IP address once connected**					
5	**Your networks are properly monitored**					
6	**Vulnerabilities are scanned on monitoring devices**					
7	**All networks are properly routed**					
8	**A good layout of cabling and devices for LAN and standard cables are used**					
9	**Banks has good network topology**					

Strongly Agree Strongly

10	Industry standard routers, hubs and switches are used and properly changed when outdated					
11	Change managements are used when changing routers or switch configurations					
12	Your bank has a good policy to connect any network devices to your LAN and activating switch ports					
13	physical space is accessed by granted user only					
14	Have policy for connecting external vendors to the LAN					
15	Physical security practiced properly for accessing premises and process for activating and deactivating badges, LAN ports and LAN connection drops.					
	Firewall and check point Questions					
1	Firewall and check point positioned properly					
2	Firewall and check point have software updates and attack signatures					

Strongly Agree Strongly

3	**All traffic that are coming to your DMZ or external and internal network are Understand and detect.**					
4	**The device has been positioned in different places on the network to understand the type of traffic that can be detected**					
5	**Firewall and check point configured properly and send an alarm to network administrator.**					

Appendix B. Interview Questions for Middle and Senior Managers

Dear sir/madam,

I am a graduate student and currently conducting a research on "Develop Multi-tiered Security architecture towards Information Infrastructure protection for Ethiopian Banking Industry" at School of Information Science, Addis Ababa University. The research is undertaken as an academic requirement of partial fulfillment of the requirements for the Degree of Master of Science in Information Systems.

As part of the research, it needs to assess the bank's current status and practice in the area of the study and you have been selected purposefully as one of the interviewees. The interview will take approximately 20 – 30 minutes to complete. Please answer each question as carefully as possible. You may decline to answer any specific question if it creates any ambiguity or any other reason. If you feel that you are not able to answer a question, then you can proceed to the next one. If you agree, the interview will be recorded, for the sole purpose of not losing any or part of your responses. Finally, I would like to confirm you that your response will be kept confidential and will be used for academic purpose only.

Thank you in advance for your kind cooperation and dedicating your time.

If you have any inquiry, please feel free and contact me at:

Email: Chamogezahegn@gmail.com

Telephone: +251910622115

Yours sincerely,

Chamo Gezahegn

1) **How Do you see information infrastructure (communication networks, associated software's and delivered services) of your banks?**

2) **Do you have any certifications that are focused on information security?**

3) **Do you have the technical know how to manage the information security systems in place?**

4) **Would you tell us your experience of monitoring the network and What threats you have observed so far?**

5) **Do you know the critical systems in your organization? What are they?**

6) **Can you confidently say your information infrastructure is effectively protected?**

7) **Would you tell us the challenges you face while ensuring Information Infrastructure Protection?**

8) **Would you Give us a high-level description of the information infrastructure?**

Appendix C. Checklist for Observation

1. **Participate in working environment where networks and systems are managed**

2. **Join in meetings and discussions at section and Directorates levels related to networks, and systems.**

3. Take a look on the configurations, accessible, of the network and systems

4. Informal discussions with vendor employees about the systems and Networks they give support for.

Appendix D: Developed Security Architecture Evaluation Questionnaire

N	MIN MAX MEAN STD.DEV					
The presentation of the architecture being in a suitable manner, its comprehensibility and coverage						
1	The Developed security architecture is understandable.					
2	The Developed security architecture is comprehensive in terms of coverage.					
3	The organization and presentation of the security					
4	The objectives of four imperatives (Strategic, T a c t i c a l , Operational & continuous improvement) is					
	The objective of the architecture is comprehensible.					
Regarding the content of the Architecture						
5	The contents of the Developed security architecture are					
6	The contents of the Developed security architecture are					
7	The contents of the Developed security architecture are complete.					
Regarding utility and applicability of the Architecture						
8	The Developed security architecture is applicable.					
9	The implementation of the Developed security architecture fits with the organization.					
10	The applicability of the Developed security architecture can improve information infrastructure protection.					

Appendix E: Interview Questions for Evaluation of the Designed Architecture

The interview aimed to get a security expert review of the proposed multi-tiered architecture that can be used for information infrastructure protection in NBE. The study highlights the following as the most critical information infrastructure in NBE; Banks' network infrastructure, Web application used for online/internet banking, Databases that contain core banking information like customer account information.

1) **Is user awareness in an organization in this case NBE important?**

2) **Is IT security personnel training important in an organization?**

3) **Is the network firewall adequate enough to protect all information infrastructure?**

4) **Are network infrastructures, application and database servers identified ideal for a bank?**

5) **Does the design have the capability to address the issue of web application and database attacks mitigation?**

6) **How effective do you think the design will be in the protection of information infrastructure?**

Appendix F: INTERVIEW TRANSCRIPTS

1) **Is user awareness in an organization in this case NBE important?**

   "Yes, the security awareness plays a key to ensure organizations information protection because the implementations of the robust security architecture without awareness can give opportunities for hackers to compromise companies resource because human are the weakest link of information security. So, the degree of awareness of the users are qualifies the organizations. For every operation, services and systems it is important for user to have knowledge that helps them to achieve the target. Awareness in a national bank of Ethiopia is very important to secure banks from cyber-attacks."

2) **Is IT security personnel training important in an organization?**

   "Yes, the skilled and knowledgeable personally are able manage company's infrastructure with understanding of his/her responsibilities. Also training give a capability for employees to operate different activities according to policies and

procedures of the banks. It also important to identify and easily fix them when it is happened."

3) **Is the network firewall adequate enough to protect all information infrastructure? "No, the traditional firewalls are not strong enough to protect advanced attacks on different systems and application like web server. The traditional firewalls are not strong enough to protect advanced attacks which targeted on core systems and databases because they have not inbuilt security features which stop them but the modern firewalls like next generation firewalls are the best one to use. So, it is recommended to use best security devices which stops the respected threats."**

4) Are network infrastructures, application and database servers identified ideal for a bank? "Yes, applications, systems and networks are very critical to the banks. Without them it is very difficult for the bank to provide services and manage their infrastructures. But with awareness of their importance all systems, devices must be UpToDate to provide the expected services. Here in the organization most of the devices are outdated and even some of them have no patch update features but they are still functioning. These devices must be replaced with the new one otherwise they can open a hole for attackers to attack banks information infrastructure."

5) Does the design have the capability to address the issue of web application and database attacks mitigation?

"Yes, the existing architectures are not fully protecting information infrastructure of the banks but the newly proposed one will be the best because they have different security features and layers and also there are a network monitory tools which manage all ups and down of systems and application with their cause. In the existing architecture they have no web and database application but on the proposed device they are WAF AND DBF. Generally, the developed architectures are the best to secure company resources from any attacks."

6) How effective do you think the design will be in the protection of information infrastructure? "On my understanding this developed multi-tiered security architectures are able to protect organizations resource from any unauthorized users and attackers by providing operational, tactical and strategic platform which are well positioned to mitigates the risk. It also helps

organizations to look over all business and technology securities and protect whenever there are any attempts.”

Running configurations of firewalls

```
ASA Version 8.4(2)
!
hostname NBE-FLO8-EF01
domain-name NBE.COM
enable password BpZSfBuKQRUG986O encrypted
names
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport access vlan 6
!
interface Ethernet0/2
!
interface Ethernet0/3
switchport access vlan 2
!
interface Ethernet0/4
switchport access vlan 7
!
interface Ethernet0/5
switchport access vlan 8
!
interface Ethernet0/6
switchport access vlan 5
!
interface Ethernet0/7
!
interface Vlan1
nameif inside2
security-level 100
ip address 10.32.0.66 255.255.255.252
!
interface Vlan2
no nameif
security-level 100
ip address dhcp
!
interface Vlan5
no forward interface Vlan1
```

nameif inside
security-level 100
ip address 10.32.0.69 255.255.255.252
!
interface Vlan7
nameif outside
security-level 0
ip address 10.32.0.77 255.255.255.252
!
interface Vlan8
no nameif
security-level 0
ip address 10.32.0.81 255.255.255.252
!
object network EXTERNAL
subnet 10.32.0.0 255.255.0.0
object network INTERNAL
subnet 10.32.0.0 255.255.0.0
!
route outside 0.0.0.0 0.0.0.0 10.32.0.78 1
route inside2 0.0.0.0 0.0.0.0 10.32.0.65 1
!
access-list IN-TO-OUT extended permit tcp any any
access-list IN-TO-OUT extended permit udp any any
access-list IN-TO-OUT extended permit icmp any any
access-list OUTSIDE-IN extended permit tcp any any
access-list OUTSIDE-IN extended permit udp any any
access-list OUTSIDE-IN extended permit icmp any any
!
!
access-group IN-TO-OUT in interface outside
access-group OUTSIDE-IN in interface inside2
object network EXTERNAL
nat (outside,inside2) dynamic interface
object network INTERNAL
nat (inside2,outside) dynamic interface
!
aaaauthentication ssh console LOCAL
!
ntp server 200.200.200.2 key 123
!
username ADMIN password BpZSfBuKQRUG986O encrypted
username admin password yksOjXLD50IyW2kA encrypted
!
class-map inspection_defeult
match default-inspection-traffic

```
!
policy-map global_policy
class inspection_defeult
inspect dns
inspect ftp
inspect h323
inspect icmp
inspect tftp
!
service-policy global_policy global
!
telnet timeout 5
ssh 10.32.0.0 255.255.0.0 inside2
ssh 10.40.0.0 255.255.0.0 inside2
ssh timeout 5
!
!
dhcpd auto_config outside
!
!
!
!
!
NBE-FLO8-EF01#
```