St. Mary's University
School of Graduate Studies

Department of Computer Science

Information and Cyber Security Risk Assessment Framework for the Banking Sector in Ethiopia

A Thesis Submitted to the Department of Computer Science of St. Mary's University in the Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

By

Biniyam Wedelu Gemeda

December, 2017

St. Mary's University
School of Graduate Studies

Department of Computer Science

Information and Cyber Security Risk Assessment Framework for the Banking Sector in Ethiopia

By Biniyam Wedelu

Panel of Examiners:

Advisor: __________________________________Signature_________________ Date__________

Internal Examiner: __________________________Signature_________________ Date__________

External Examiner: __________________________Signature_________________ Date_______

Table of Contents

Abstract

In the modern banking industry information technology is playing a great role to facilitate the service and to make it competent. The competencies between banks stared on the advancement of information technology. The more implementing Information Technology the more to be vulnerable to attacks from inside or outside of the organization.

The main objective of this research work is to assess the banks information security risk and developing a risk assessment framework. The researcher has sampled six private and public banks in Ethiopia to survey their information security culture and assessing the risk the banks confronted and facing currently.

The methodologies used in this research are both quantitative and qualitative methodologies. Through distributing questionnaire and interviewing to Information Technology top managers, security officials, and system and network administrators' huge amount of data has been collected. These data has been further complemented by making site surveys. Risk Management studio was used to assess the risk and to identify threats.

After assessing the banks risk conclusion are drawn that are used as inputs for the new framework. The proposed framework was designed and developed from the findings of literature review and survey methods. The framework has eleven components such as: - identify the scope of the system asset identification, parameter identification, threat identification, relating threat with vulnerability, vulnerability analysis, possibility study, impact study, risk prioritization, evaluation, communication, and documentation stages.

Key-words: Risk Assessment, Risk Assessment Framework, Risk Management and Information Security.

DECLARATION

I, Biniyam Wedelu Gemeda, hereby declare that the thesis work entitled “Information and Cyber Security Risk Assessment Framework for the Banking Industry in Ethiopia” is my own original work.

Name………………………………

Date ………………………………..

Signature……………………………

ACKNOWLEDGEMENTS

Primarily, next to God, I would like to express my sincere gratitude to my advisor Ato. Asrat Mulatu: for his continuous support, patience and motivation. His guidance helped me in all the time while conducting this thesis work.

It is my pleasure to thank the surveyed banks IT managers, information security experts and officials who gave me their precious time to respond to my questionnaires, answer my questions and collaborate with me during site survey, data collection and validation phases.

Lastly, my genuine appreciation goes to my families and friends because they were always by my side.

Biniyam Wedelu

List of Acronyms

ATM	Automatic Tailor Machine
CCTV	Closed Circuit Television
COBIT	Control Objectives for Information and Related Technology
DDoS	Distributed Denial of Service
EEU	Ethiopian Electric Utility
ERM	Entity Relationship Model
ICSRAF	Information and Cyber Security Risk Assessment Framework
IS	Information System
ISO	International Standard Organization
IT	Information Technology
MSAT	Microsoft Security Assessment Tool
NBE	National Bank of Ethiopia
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
RA/RM	Risk Assessment/Risk Management
RAF	Risk Assessment Framework
RM Studio	Risk Management Studio
UK	United Kingdom
US	United States

List of Figures

List of Tables

List of Appendixes

CHAPTER ONE

INTRODUCTION

1.1 Background

Information is considered as an asset like other important business assets and Information Security (IS) is a way of protecting information from a wide range of threats in order to ensure business continuity, minimize risk, and maximizes return on investments and business opportunities. Over the years the usage of Information Technology (IT) has increased massively in organizations and in societies and to provide the ever increasing requirement of information flow, information systems has become complex and multifaceted. IT has made electronic communication and Internet mandatory in all organizations. This necessity has brought efficiency and also threats of hacking and intrusion with it .

With all these advancements in the field of IT, dependency of organizational business functionality on IT has increased the requirements of securing organizational information from threats; one of the prime reasons that not much data related to information security management and threats to organizations is available due to confidentiality. Second, costs associated to information security discourage organizations from implementing information security management systems in organizations . Third, information security is not just a technical issue, it is more of managerial issue, Therefore, it is also required to train employees about the information security without which attaining information security is Impossible [1].

Organizations adopt information security products, services, processes and tools. Organizations are not sure about the optimal security requirements. They need cost effective information security methods which can provide them optimal security with minimum cost [1]. Knowledge sharing and collaboration of intra organizational cross functional teams for risk management is required for proper risk management strategies [1] .Management vision towards information security risk and involving internal stakeholder in this task is the need of the time. A more pragmatic reason is that the development of information security methods within organizations is rather an ad hoc process than a systematic one. This research will generate new knowledge about information security risk management by constituting valuable organizational intelligence.

Risk assessment is the careful analysis and evaluation of the diverse factors that can bring risks. It provides for the banks an opportunity to determine the vulnerabilities and risk associated with a banking system. The significance of risk assessment is obvious once a risk management system is developed and management wants to recognize the effectiveness of such a system. It’s an important step of risk management in protecting the business from losses.

In Ethiopia, commercial banks are playing an important role as financial intermediaries in the economic growth process, channeling funds from savers to borrowers for investment. In such away, commercial banks are key providers of funds and their stability is of paramount importance to the financial system [2]. So it is important that understanding the determinants of managerial efficiency which has impact on banks profitability useful for success of the banks in state owned and private banks. This is the reason for which this research focus on assessing the effects banking risks on operating efficiency of Ethiopian commercial banks industry by using both primary and secondary data.

1.1.1 Vulnerability Analysis

The purpose of vulnerability analysis is to take what was identified in the gathering of information and test to determine the current exposure, whether current safe guards are sufficient in terms of confidentiality, integrity or availability. It will also give an indication as to whether the proposed safe guards will be sufficient.

1.1.2 Threat Analysis

Threats can be described as anything that would contribute to the tampering, destruction or interruption of any service or item of value. The analysis will look at every element of risk that could conceivably happen. These threats can be split into Human and Non-human elements. As shown in Table 1.1.

Table 1.1: Threat Analysis

Human	Non-human
• Hackers • Theft (electronically and physically) • Non-technical staff (financial/accounting) • Accidental Inadequately trained IT staff • Backup operators • Technicians, Electricians	• Viruses • Fire • Electrical • Heat control • Air (dust) • Flood

1.1.3 Risk Categorization

It is proposed to categorize risks according to their impact and level of consequences and it is going to be categorized as shown below in.

Table 1.1: Risk Categorization

L = Low	Low risks and low consequences that may be managed by routine procedures
M = Medium	Medium risks that are likely to arise or have serious consequences requiring attention
H = High	High risks that are likely to arise and have potentially serious consequences requiring attention an investigation.
E = Very high	Extreme risks those are likely to arise and have potentially serious consequences requiring immediate action.

1.2 Statement of the Problem

In response to the facts that the computer network of banks has multiple trading channels, the system is quite open and system data can be concentrated, banks and the government have followed identical network security mechanisms. This research intends to assess the information system and cyber security of Ethiopian banks, makes implementable techniques of the security and establishes an assessment model of information system security for the banking sector in general.

In recent years, security ambiguity becomes visible. For example, deposit is missing for no reasons and bank credit card becomes invalid [3]. All these worry people a lot. Many banks recruited professionals to assess the computer network security in order to avoid unnecessary losses. Thus, it is important to conduct risk assessment of information and cyber security risk of banks, as it can increase the security level of banks, guarantees normal operation maintains bank's reputation and promotes a normal and stable life.

There is no agreement on how information and cyber related risks are impacting the operating efficiency or performance of banks since different studies provide different findings and no specific research has been done assessing cyber and information security risks in Ethiopian banks [4].The financial institutions operate in a very uncertain environment where conditions can change due to Internet connection speed, user over flow, network congestion, network failure, government influence and electric power inconsistency.

Advancements in IT have exposed banks and financial institutions to information security threats, several methods and standards for assessment of information security in an organization are available today. Different threats and vulnerabilities are following these developments, assessing risks which will cause a loss and company image destruction is a very crucial issue. In this research it is going to assess these threats and implicate episodes the organizations should follow to make their business run safely and swim in a secure pool of information.

In Ethiopia, banking industry has been facing a lot of obstacles regarding information and cyber security attacks [5].These banks doesn’t have a platform to assess these risks to identify and prioritize threats and to measure the likelihood of the threats.

Even though there is locally developed cyber security framework it is merely focused on the organizational structure and application of cyber security risk assessment not intensely designed to do a risk assessment. This framework basically is developed for only cyber security not information and cyber security.

1.3 Research Questions

This research is conducted to answer questions which might be raised in the banking industry in Ethiopia. Such as:-

- What information and cyber security risk assessment practices are engaged in Ethiopian Banks?
- How is the likelihood of these attacks?
- How should the banking sector strategy for prioritizing and sharing information about the security risks to an information technology (IT) infrastructure.
- What kind of ICS (Information and Cyber Security) framework is needed for the banking sector in Ethiopia?

1.4 Research Objectives

The report has its general and specific objectives such like:

1.4.1 General Objectives

The objective of this research is to identify risks through analysis of the information/data collected and develop a risk assessment framework. It is also planned to forward remedies based international standards and industry recommendations.

1.4.2 Specific Objectives

- To examine the banks information and cyber risk management environment. .
- To analyze assets, threats and vulnerabilities, including their impacts and likelihood.
- To develop practical technical recommendations to address the vulnerabilities identified, and reduce the level of security risks.
- To develop a conceptual risk assessment framework for Ethiopian private and public banks.

1.5 Significance of the Research

The researchers' believe is that this study has the following significance for different parties.

- A practical risk assessment program is important to supporting an organization's business activities and provides several benefits:
- Risk assessment helps to ensure the maximum risks for the organization to be identified and addressed on a continuing basis. Thus, it will create a reasonable step for preventing or mitigating situations that could interfere with accomplishing the organization's mission.
- Risk assessments provide a mechanism for reaching a consensus as to which risks are more harmful and what steps are appropriate for mitigating them. The processes used encourage discussion and generally require that disagreements be resolved.
- It provides a basis for future comparisons of changes made in Information security measures.
- It enables all banks to have a common ICS framework in Ethiopia.
- It may also serve as a starting point for practitioners and researchers who want to conduct more comprehensive research in this area from Ethiopian banking sector perspective.

1.6 Scope of the Research

The research mainly focuses on some competitive banks in Ethiopia and it will inclusively consider private and government owned banks. Because there are various private banks in our country it is better to chose randomly as a target working area.

1.7 Limitations of the Study

The result of the research would be more comprehensive if it covers the entire Banks in Ethiopia. However, due to financial and time limitations, it is enclosed to head quarter of some sample Banks in Addis Ababa. The head quarter is a place where major information, cyber security resources and facilities resides and the offices of IT staffs are sited.

1.8 Thesis Organization

The rest of this thesis report is organized as follows:

Chapter One: introduces what ICSRA is and how the risk is assessed using existing frameworks.

Chapter Two: is the part where literature on information security, cyber security ICSRA and how ISCRAF is developed.

Chapter Three: this chapter presents research design and methodology which includes general insight on the existing research methods, what research method was employed in this thesis and why? Moreover, selection of sample for the study, data collection techniques, and data analysis methods was stated clearly.

Chapter Four: here the data collected through questionnaire, interview, and document collection was analyzed and presented. And the findings from the analysis were discussed, interpreted and summarization was made as related to the research problems stated.

Chapter Five: is the part where a new proposed ISCRA Framework is clearly presented.

Chapter six: is the unit where evaluation and comments by sampled banks officers is clearly stated.

Chapter Seven: is the chapter where concluding remarks and recommendations were made.

CHAPTER TWO

LITERATURE REVIEW

In this chapter, the researcher has tried to review the background of information and cyber security and its theoretical and empirical framework for designing and implementing ICSRA framework in a bank. The reviewed points are focused on Information and security, cyber security, information and cyber security risk assessment, information and cyber security risk assessment frameworks.

2.1 Information security

As stated in [6], information is one of financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institutions and its customers, to maintain compliance with the law, and to protect the reputation of the institution itself. Timely and reliable information is necessary to process transactions and support financial institution to make related customer decisions.

The enterprise risk assessment and enterprise risk management processes comprise the heart of the information security framework. These are the processes that establish the rules and guidelines of the security policy while transforming the objectives of an information security framework into specific plans for the implementation of key controls and mechanisms that minimize threats and vulnerabilities [5].

A financial institution's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed. Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintains information vital to its operations [7].

On a broad scale, the banking industry in Ethiopia has a primary role in protecting the nation's financial services infrastructure and the security of the industry's systems and information is essential to its safety and soundness and to the privacy of customer financial information. Individual financial institutions and their service providers must maintain effective security programs adequate for their operational complexity [4]. These security programs must have strong top management level support, integration of security activities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities.

Three basic security concepts are important to the information such as confidentiality, integrity, and availability. Concepts related to individual who use that information are authentication, authorization, and non-repudiation [8].

When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Examples include credit card data, personnel and insurance records, new product specifications, and corporate investment strategies. In some locations, there might be a legal obligation to protect the privacy of individuals. This is particularly right for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; and organizations that collect taxes [9].

Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic money transfers, and financial accounting [10].

Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need [1]. Availability is often the most important attribute in financial institutions that depend on information, for example, mobile banking and online inventory systems.

In the financial institutions, as [1] described, to make information available to those who need it and who can be trusted with it, most of them use authentication and authorization. Authentication is proving that a user is the person he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a "visa card"), or something about the user that proves the person's identity (such as a fingerprint). Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program.

In financial institutions Authentication and Authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted; the user cannot later deny that he or she performed the activity [11].

Therefore:-

- Users can trust the information they use
- The information they are responsible for will be shared only in the manner that they expect
- The information will be available when they need it and
- The systems they use will process information in a timely and trustworthy manner

In addition, information assurance extends to systems of all kinds, including large scale distributed systems, control systems, and embedded systems, and it encompasses systems with hardware, software, and human components [12].

2.1.1 Attacks in Financial Industries

In most financial institutions attacks held in different ways because the vulnerability to get attacked is higher because financial institutions advancement and competition is stared at IT achievement like mobile banking, mobile agent, ATM and Internet banking [6]. Attacks which are recognized in most financial institutions are presented as [6]:-

Denial of service attack: Unlike other exploits, denials of service attacks are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering wrong password consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. These types of attack are, in practice, very hard to prevent, because the behavior of the whole network needs to be analyzed, not only the behavior of small pieces of code. Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers", used as part of a botnet with, for example; a worm, Trojan horse, thus attempting to render it unusable through resource exhaustion [6].

Direct access attack: An unauthorized user gaining physical access to a computer (or part thereof) can perform many functions; install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CDR, DVD, tape; or portable devices such as key drives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD ROM or other bootable media and read the data from the hard drive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system [13].

Eavesdropping: is the act of surreptitiously listening to a private conversation, typically between hosts on a network [13].

Spoofing: Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Information disclosure: (Privacy breach or Data leak) describes a situation where information, thought as secure, is released in an entrusted environment.

Elevation of privilege: describes a situation where a person or a program want to gain elevated privileges or access to resources that are normally restricted to him or her.

Exploits: An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a software "bug" or "glitch" in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack. The term "exploit" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in Trojan horses and computer viruses.

Indirect attacks: An indirect attack is an attack launched by a third party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public systems, such as the tor onion router system.

2.1.2 Vulnerability

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. It is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface [3].

2.2 Cyber Security

In the last 10 years, digital technology has revolutionized economic and social interaction [8]. It has transformed the way peoples do business, the way people educate themselves, the way people sell and buy products and the way people share data. Internet use is growing and the methods by which it is accessed are diversifying. Malicious cyber actors are fully aware of this revolution and are taking full advantage of it. Organizations have indicated that: 2013 saw an exponential increase in cyber-attacks and recent surveys demonstrates that 93% of large organizations last year suffered a security breach [14].

The targeted intrusion into a bank's systems is often perceived as the greatest threat due to the malicious actor's ability to not only steal data but modify or delete it. By exploiting software, hardware or human vulnerabilities hackers can gain administrative control of networks which, if abused, could cause disastrous consequences. If publicized, network security breaches can affect share prices, cause irreparable reputational damage and impact on the stability of the wider financial market.

2.3 Information and Cyber Security Risk Assessment Related Works

Information security is all about protecting ones organization data (physical or digital) from attack, Cyber security is the subset of information security which deals with protecting organizations network, computers, and data from unauthorized digital access or attack or damage by implementing different practices technologies and policies.

Risk is the potential harm that may arise from some current process or from some future event. It is present in every aspect of our lives and many different disciplines focus on risk as it applies to them. From the IT security perspective, risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. IT security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or related information [15].

The quality of security controls can significantly influence all categories of risk. Traditionally examiners and institutions recognized the direct impact on operational (transaction) risk from incidents related to fraud, theft, or accidental damage. Many security weaknesses, however, can directly increase exposure in other risk areas [15]. The potential for legal liability related to customer privacy breaches may present additional risk. Effective application access controls can strengthen credit and market risk management by enforcing risk limits on loan officers or traders. For example, if a trader were to exceed the intended trade authority, the institution may unknowingly assume additional market risk exposure.

A strong security program reduces levels of reputation, operational, legal, and strategic risk by limiting the institution's vulnerability to intrusion attempts and maintaining customer confidence and trust in the institution. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services. Examiners and risk managers should incorporate security issues into their risk assessment process for each risk category.

Financial institutions should ensure that security risk assessments adequately consider potential risk in all business lines and risk categories. Information and cyber security risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems [7].

In its simplest form, a risk assessment consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information should be used to develop strategies to mitigate those risks. An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities.

A risk assessment is a pre requisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security attitude. An initial risk assessment may involve a significant one time effort, but the risk assessment process should be an ongoing part of the information security program. Risk assessments for most industries focus only on the risk to the business entity. Financial institutions must also consider the risk to their customers' information. For example, guidelines require financial institutions to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer [12].

Most of the time, people get confused that information security and cyber security are both the same but they have a slight difference information security (data security) is concern of data integrity, confidentiality, and availability of electronic data weather it is an electronic or not, whereas, cyber security is protecting data which are presented in an electronic form [16].

As [17] stated that, in our country there are no formally developed cyber security frameworks but as he tried to develop these problems he tried to design and develop a framework which is helpful to apply cyber security risk assessment he has used critical mass cyber security requirements standards as an insight. This framework is requirement standard to perform risk assessment in strategic and tactical level.

2.3.1 Assessing Risk

Assessing risk is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise. When assessing the likelihood and impact, just by taking the current threat environment and controls into consideration. Likelihood and impact are assessed on the system as it is operating at the time of the assessment [17].

2.3.2 How is Risk Assessed?

As Underlined in [17], Risk is assessed by identifying threats and vulnerabilities, determining the likelihood and the impact for each risk. Unfortunately, risk assessment is a complex undertaking, usually based on imperfect information. There are many methodologies aimed at allowing risk assessment to be repeatable and give consistent results. Some of the leading methods are discussed below.

2.3.2.1 Quantitative Risk Assessment

Quantitative risk assessment draws upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, business processes etc., impact, and therefore risk, can be measured in terms of direct and indirect costs.

As mathematically described in [7], quantitative risk can be expressed as Annualized Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realized over a one year period.

$$ALE = SLE * ARO \text{……………………………………Equation 2.3-1}$$

Where:

- SLE (Single Loss Expectancy) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss.
- ARO (Annualized Rate of Occurrence) is how often the loss occurs. This is the likelihood.

While utilizing quantitative risk assessment seems straightforward and logical, there are issues with using this approach with information systems [7]. While the cost of a system may be easy to define, the indirect costs, such as value of the information, lost production activity and the cost to recover is imperfectly known at best. Moreover, the other major element of risk, likelihood, is often even less perfectly known. For example, what is the likelihood that someone will use social engineering to gain access to a user account on the accounting system? Therefore, a large margin of error is typically inherent in quantitative risk assessments for information systems.

As the body of statistical evidence becomes available, trends can be extrapolated on past experience. Insurance companies and financial institutions make excellent use of such statistics to ensure that their quantitative risk assessments are meaningful, repeatable and consistent [18].

Typically, it is not cost effective to perform a quantitative risk assessment for an IT system, due to the relative difficulty of obtaining accurate and complete information. However, if the information is deemed reliable, a qualitative risk assessment is an extremely powerful tool to communicate risk to all level of management. Quantitative risk measurement is the standard way of measuring risk in many fields, such as insurance, but it is not commonly used to measure risk in information systems. Two of the reasons claimed for this are 1) the difficulties in identifying and assigning a value to assets, and 2) the lack of statistical information that would make it possible to determine frequency. Thus, most of the risk assessment tools that are used today for information systems are measurements of qualitative risk [19].

2.3.2.2 Qualitative Risk Assessment

Qualitative risk assessments assume that there is already a great degree of uncertainty in the likelihood and impact values and defines them, and thus risk, in somewhat subjective or qualitative terms. Similar to the issues in quantitative risk assessment, the great difficulty in qualitative risk assessment is defining the likelihood and impact values. Moreover, these values need to be defined in a manner that allows the same scales to be consistently used across multiple risk assessments.

The results of qualitative risk assessments are inherently more difficult to concisely communicate to management. Qualitative risk assessments typically give risk results of “High”, “Moderate” and “Low”. However, by providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization’s management [11].

In a qualitative risk assessment, it is best not to use numbers when assessing risk. Managers, especially the senior level managers that make decisions concerning resource allocation, often assume more accuracy than is actually conveyed when reviewing a risk assessment report containing numerical values. in a qualitative risk assessment, the likelihood and impact values are based on the best available information, which is not typically well grounded in documented past occurrences. The concept of not providing any more granularity in risk assessment reports than was available during the assessment process is roughly analogous to the use of significant digits in physics and chemistry. Roughly speaking, significant digits are the digits in a measurement that are reliable. Therefore, it is impossible to get any more accuracy from the result than was available from the source data. Following this logic, if likelihood and impact were evaluated on a Low, Moderate, High basis, Risk would also be Low, Moderate or High [11].

2.3.2.3 Risk Assessment Techniques

In [10] there are a variety of risk assessment techniques are discussed which can be applied at different stages of the decision process. These range from high level methods to intermediate methods to detailed methods. Screening and prioritization methods rely heavily on engineering judgment, even as fully qualitative methods may involve full probabilistic analysis. Between these extremes there are a range of generic quantitative methods which are presented as:-

I. Brainstorming

When objectives are stated clearly and understood by the participants, a brainstorming session drawing on the creativity of the participants can be used to generate a list of risks. In a well facilitated brainstorming session, the participants are collaborators, comprising a team that works together to articulate the risks that maybe known by some in the group. In the session, risks that are known unknowns may emerge, and perhaps even some risks that were previously unknown unknowns may become known. Facilitating a brainstorming session takes special leadership skills, and, in some organizations, members of the internal audit and ERM (enterprise resource management) staffs have been trained and certified to conduct risk brainstorming sessions [10].

II. SWOT Analysis (strengths weaknesses opportunities threats)

It is a technique often used in the formulation of strategy The strengths and weaknesses are internal to the company and include the company’s culture, structure, and financial and human resources. The major strengths of the company combine to form the core competencies that provide the basis for the company to achieve a competitive advantage. The opportunities and threats consist of variables outside the company and typically are not under the control of senior management in the short run, such as the broad spectrum of political, societal, environmental, and industry risks [10].

III. Questionnaire

A risk questionnaire that includes a series of questions on both internal and external events can also be used effectively to identify risks. For the external area, questions might be directed at political and social risk, regulatory risk, industry risk, economic risk, environmental risk, competition risk, and so forth. Questions on the internal perspective might address risk relating to customers, creditors investors, suppliers, operations, products, production processes, facilities, information systems, and so on.

Questionnaires are valuable because they can help a company think through its own risks by providing a list of questions around certain risks. The disadvantage of questionnaires is that they usually are not linked to strategy. Rather than a lengthy questionnaire, a risk survey can be used. In one company, surveys were sent to both lower and senior level management [1].

IV. Interview

This technique combines two different processes. First, each individual of the organizational or operating units is given a template with instructions to list the key strategies and objectives within his or her area of responsibility and the risks that could obstruct the achievement of the objectives [20].

2.4 Risk Assessment Tools

Even though there are enormous tools and techniques to assess and manage risks they are different in their specification and requirement. As a result, comparing these tools and methodologies is vital.

2.4.1 Comparison of Risk Assessment Tools and Techniques

There are several models and methods with different approaches that aid in the risk assessment process [21].There are several methods and tools that can support the risk assessment process and those which can be applied to information security. Risk assessment models can be separated into quantitative and qualitative. Below the tables compare Information Security Risk Assessment methods and a comparison that evaluates those different methodologies [21]. It aims to describe and compare properties of Information Security Risk Assessment methods in a concise manner.

Table 2.4: Comparing Risk Assessment Tools: Quantitative vs. Qualitative

QUANTITATIVE	QUALITATIVE
Risks are prioritized by financial impact; assets are prioritized by financial values.	Enables visibility and understanding of risk ranking.
Results facilitate management of risk by return on security investment.	Easier to reach consensus
Results can be expressed in management specific terminology (for example, monetary values and probability expressed as a specific percentage	Not necessary to quantify threat frequency.
Calculations can be complex and time consuming	Not necessary to determine financial values of assets.
Accuracy tends to increase over time as the organization builds historic record of data while gaining experience	Easier to involve people who are not experts on security or computers.

Table 2.4: Comparing Risk Assessment Tool Based on Their Characteristics

Tools	Identify ISC Risks	Forums	Update	Required skill	Price/license (€)
OCTAVE	yes	Yes	Up to date	Standard	Free
Acuity Stream	yes	Yes	Up to date	Basic	Free
Callio secura 17799	yes	Yes	Up to date	Basic	2.250
CCS Risk Manager	yes	Yes	Up to date	Standard	227.330
CORAS Tool	yes	Yes	Up to date	Standard	Open source
Countermeasures	yes	Yes	Up to date	Standard	350
CRAMM expert	yes	Yes	Up to date	Advanced	4413
CRAMM express	yes	Yes	Up to date	Basic	2000
EAR/PILAR	yes	Yes	Up to date	Basic	1500
Ebios tool	yes	Yes	Up to date	Standard	Open source
FAIR lite	yes	Yes	Up to date	Basic	Free
GS Tool	yes	Yes	Up to date	Basic	887
HiScout GRC Suite	yes	Yes	Up to date	Standard	On request
Mehari 2010 basic tool	yes	Yes	Up to date	Standard	Open source
Modulo Risk Manager	yes	Yes	Up to date	Standard	On request
MSAT	yes	Yes	Up to date	Basic	Free
Proteus Enterprise	yes	Yes	Up to date	Advanced	694
Resolver Ballot	yes	Yes	Up to date	Standard	1300
Risicare	yes	Yes	Up to date	Standard	On request
Riskwatch	yes	Yes	Up to date	Standard	14000
RM Studio	yes	Yes	Up to date	Standard	On request
SAVe	yes	Yes	Up to date	Standard	800
TRICK light	yes	Yes	Up to date	Standard	On request
Verinice	yes	Yes	Up to date	Basic	Open source
VsRisk	yes	Yes	Up to date	Standard	1323

Tools are software which can help researchers to analyze risks and threats. But guideline is a document which is use full to advice or instructions in order to guide or direct an action. A standard is a set of rules widely recognized or engaged (especially because of its excellence) that control how people develop and manage materials, products, services, technologies, tasks, processes, and systems. Many researchers have used both guidelines and tools to come up with a concrete decision.

As [1] has shown, tools and methodologies to perform risk assessment and risk management have a wide concerning area of study. In the above Table 5.1 Comparing Risk assessment tools to measure risk and manage risk are a bit expensive and they are not available easily.

Though, some tools are designed for security critical systems, while others are created with certification in mind [14]. Some tools are expensive and can only be used by experts while others are free and easy to use. Some frameworks are overly complex and only suitable for large project and organizations while others can be implemented by a few skilled employees. Such criteria can be used to not only classify and understand the scope, applicability and benefits offered by each methodology, framework and tool, but also as indicators for choosing the most appropriate resource for any environment and protection requirements. As such, guidelines, similar to the ones introduced in can be designed and used to shed some light on the plethora of Risk Assessment and Risk Management frameworks, methods and tools.

Table 2.4: Comparing Risk Assessment Tools based on Their Feature

TOOLS	FEATURES									
	Risk identification	Risk analysis	Risk evaluation	Risk treatment	Risk communication	Risk control mapping	Asset categories catalog	Treat and vulnerability library	Comparing results	Built in report
OCTAVE	Yes	Yes	Yes	yes	Yes	yes	Yes	yes	No	Yes
ACUTy	Yes	Yes	Yes	yes	Yes	no	No	yes	Yes	yes
Callio rm	Yes	No	Yes	yes	Yes	no	No	yes	Yes	Yes
Scura CCS	Yes	Yes	Yes	yes	Yes	yes	No	yes	Yes	Yes
CORAS too	Yes	Yes	Yes	yes	Yes	yes	No	No	Yes	Yes
CRAMM expert	Yes	Yes	Yes	yes	Yes	yes	No	No	Yes	Yes
CRAMM	Yes	Yes	Yes	yes	Yes	yes	No	No	N/A	Yes
EAR/PILLAR	Yes	Yes	Yes	yes	Yes	yes	No	yes	No	Yes
Ebios	Yes	Yes	Yes	yes	Yes	yes	No	yes	No	Yes
FAIRlite	Yes	Yes	Yes	No	No	NO	No	N/A	No	Yes
GST	Yes	Yes	Yes	yes	Yes	N/A	No	N/A	No	Yes
Hiscout GRC	Yes	Yes	Yes	yes	Yes	N/A	No	N/A	No	Yes
MEHARI	Yes	Yes	Yes	yes	N/A	N/A	No	N/A	No	yes
MODULO	Yes	Yes	Yes	yes	Yes	N/A	No	N/A	No	Yes
MSAT	Yes	Yes	Yes	NO	NO	Yes	Yes	N/A	N/A	yes
PROTEUS ENT.	Yes	Yes	Yes	yes	Yes	N/A	No	N/A	N/A	No
RESOLVER BALLOT	Yes	Yes	Yes	NO	NO	N/A	No	N/A	N/A	yes
RISICARE	Yes	Yes	Yes	yes	Yes	N/A	No	N/A	NO	yes
RISK WATCH	Yes	Yes	Yes	yes	NO	N/A	No	N/A	NO	yes
RM studio	Yes	Yes	Yes	yes	Yes	Yes	Yes	Yes	Yes	yes
SAVe	Yes	Yes	Yes	yes	Yes	N/A	No	No	NO	yes
Trick light	Yes	Yes	Yes	yes	Yes	N/A	No	N/A	NO	yes
Verinice	Yes	Yes	Yes	LIMITED	NO	N/A	No	N/A	NO	yes
VS Risk	Yes	yes	Yes	yes	Yes	N/A	No	N/A	N/A	N/A

The above table shows that most tools claim to provide support for all the steps like risk identification, analysis, evolution treatment and communication. However, only a few software tools available actually cover all the steps required for performing an entire assessment solely within the application (e.g. Acuity Stream, CCS Risk Manager, EAR/PILAR, GSTool, Modulo Risk Manager, Proteus, RiskWatch, RM Studio). Others are only useful for automating or facilitating certain sub processes or activities (e.g.

vsRisk, Resolver Ballot, FAIRiq, FAIRlite and TRICKlight, CRAMM for Risk Assessment process, MEHARI basic tool for Risk Analysis process.

Accordingly, among these the above listed and analyzed Risk assessment tools it is concluded that using RM studio will make the result outcomes more efficient and reliable. Because it contains all features which are itemized as a criteria for comparison in the above Table.

2.5 Information and Cyber Security Risk Assessment in the Banking Industry

Risk management is critical for any financial firm. As security and regulatory compliance are central to managing risk, integrating security and compliance capabilities into the enterprise architecture should be a significant part of a firm's technology priorities.

Cyber security threats impose direct costs on financial institutions such as banks and insurance companies. Those costs include loss of funds or customer records, added IT spending, remediation costs, reputation costs, and legal expenses.

Cyber security incidents also can pose a broader risk to financial stability. Financial organizations work within complex networks and rely on electronic transactions, often on a rapid just in time basis. They are linked digitally to each other and to nonfinancial entities, including third party service providers. Some markets and systems depend on a few key organizations [22]. Other markets and systems may be decentralized, either by design or because participation is not concentrated. Hackers may have a hard time spreading chaos in those operations. However, defending a decentralized network with many entry points can be difficult.

In banking systems numerous attacks and breaches occur in different aims. Defending and countering cyber-attacks at the same time as keeping up to date with evolving regulations and policy is a complex challenge. Coupled with changing business requirements, speed to market pressures, expansion into emerging markets, business innovation requirements and budget cuts, the challenge for managing cyber risk is significant organizations are already investing heavily in cyber security. The UK financial sector is already spending over £700 million annually. The issue is also being managed at board level; with 86% of banking and capital market top level managers identifying technological advances as the trend that will have greatest impact on their businesses [22].

Cyber and information attacks against financial services institutions like banks are becoming more frequent, more sophisticated, and more widespread. Although large scale denial of services attacks against major financial institutions generate the most headlines, community and regional banks, credit unions, money transmitters, and third party service providers such as credit card and payment processors have experienced attempted breaches in recent years [4].

The rise in frequency and breadth of cyber-attacks can be attributed to a number of factors. Unfriendly nation states breach systems to seek intelligence or intellectual property. Hacktivists aim to make political statements through systems disruptions. Organized crime groups, cyber gangs, and other criminals breach systems for monetary gain i.e., to steal funds via account takeovers, ATM heists, and other mechanisms. As the cost of technology decreases, the barriers to entry for cyber-crime drop, making it easier and cheaper for criminals of all types to seek out new ways to perpetrate cyber fraud [3].

Most researches which are done in banking industry information and cyber risk assessment lacked a qualitative methodology, most of these papers and researches go around using quantitative methodologies [6] have used quantitative methodology and COBRA tool to analyze their data.

2.5.1 Identifying Threats

In risk assessment processes both threat sources and threats must be identified. Threats should include the threat source to ensure accurate assessment. Some common threat sources include [23]:

- Natural threats floods, earthquakes, hurricanes
- Human threats caused by human beings, including both unintentional (in advertent data entry) and deliberate actions (network based attacks, virus infection, and unauthorized access)
- Environmental threats like power failure, pollution, chemicals, and water damage

Hence, it is valuable to compile a list of threats that are present across the organization and use this list as the basis for all risk management activities. As a major consideration of risk management is to ensure consistency and repeatability, an organizational threat list is invaluable.

2.5.2 Identifying Vulnerabilities

Vulnerabilities can be identified by numerous means. Different risk management schemes offer different methodologies for identifying vulnerabilities. In general, start with commonly available vulnerability lists or control areas. Then, working with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system. If they exist, previous risk assessments and audit reports are the best place to start [18].

- Vulnerability Scanners – Software that can examine an operating system, network application or code for known flaws by comparing the system to a database of flaw signatures.
- Penetration Testing – An attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering
- Audit of Operational and Management Controls – A thorough review of operational and management controls by comparing the current documentation to best practices and by comparing actual practices against current documented processes. It is invaluable to have a base list of vulnerabilities that are always considered during every risk assessment in the organization. This practice ensures at least a minimum level of consistency between risk assessments. Moreover, vulnerabilities discovered during past assessments of the system should be included in all future assessments. Doing this allows management to understand that past risk management activities have been effective [18].

2.5.3 Relating Threats to Vulnerabilities

One of the more difficult activities in the risk management process is to relate a threat to vulnerability. Nonetheless, establishing these relationships is a mandatory activity, since risk is defined as the exercise of a threat against vulnerability. This is often called threat vulnerability pairing. Once again, there are many techniques to perform this task. Not every threat action or threat can be exercised against vulnerability [12].

While logically it seems that a standard set of threats and vulnerability pairs would be widely available and used; there currently is not one readily available. This may be due to the fact that threats and especially vulnerabilities are constantly being discovered and that the TV (threat and vulnerability) pairs would change fairly often. Nonetheless, an organizational standard list of TV (threat and vulnerability) pairs should be established and used as a base line. Developing the TV pair list is accomplished by reviewing the vulnerability list and pairing vulnerability with every threat that applies, then by reviewing the threat list and ensuring that all the vulnerabilities that that threat action threat can act against have been identified. For each system, the standard TV pair list should then be tailored [7]- [12].

2.5.4 Defining Likelihood

Determining likelihood is fairly straightforward. It is the probability that a threat caused by a threat source will occur against vulnerability. In order to ensure that risk assessments are Consistent, it is an excellent idea to utilize a standard definition of likelihood on all risk assessments [24].

In order to ensure repeatability, impact is best defined in terms of impact upon availability, impact upon integrity and impact upon confidentiality. However, in order to be meaningful, reusable and easily communicated, specific ratings should be produced for the entire organization.

2.6 Information and Cyber Security Risk Assessment Frameworks

As defined in [25] “Framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful”. The above definition of framework is used as reference in this paper because it is more comprehensive and suitable for this research work.

The sensitivity of a risk assessment framework is an objective, repeatable methodology that gathers input regarding business risks, threats, vulnerabilities, and controls and produces a risk scale that can be discussed, reasoned about, and treated. The various risk frameworks follow similar structures, but differ in the description and details of the steps. However, they all follow the general pattern of identifying assets and stakeholders, understanding security requirements, counting threats, identifying and assessing the effectiveness of controls, and calculating the risk based on the inherent risk of compromise and the likelihood that the threat will be realized.

A good RAF organizes and presents information in a way that both technical and non-technical personnel can understand. It has three important components: a shared vocabulary, consistent assessment methods and a reporting system [26]. The common view and RAF provides and helps an organization see which of its systems are at low risk for abuse or attack and which are at high risk. The data an RAF provides is useful for addressing potential threats pro-actively, planning budgets and creating a culture in which the value of data is understood and appreciated.

The most widely used RAF has been designed and developed by these three organizations:-

- Risk Management Guide for Information Technology Systems (NIST guide) from the National Institute of Standards.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) from the Computer Emergency Readiness Team.
- Control Objectives for Information and related Technology (COBIT) from the Information Systems Audit and Control Association.

- ISO 270001 standards

2.6.1 Risk Management Guide for Information Technology Systems (NIST guide)

NIST 800-30 is the US government's preferred risk assessment methodology, and is mandated for US government agencies. It features a detailed step by step process from the initial stages of preparing for an assessment, through conducting it, communicating the results, and maintaining the assessment. Unsurprisingly, as a US standard, much of the supporting documentation in the NIST Risk Management Framework is heavily US-focused, often residence on regulatory issues.

A weakness of the NIST framework is its lack of focus on any financial aspects, which may make some people withdrawn away from utilizing the NIST documentation [15]. Individuals need to know what they are looking for when they begin searching the NIST catalog, so they do not spend time reading non-pertinent information due to the amount of information available.

2.6.2 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology originates from Carnegie Mellon University in the USA. Older versions are still in use but the most recent version, OCTAVE Allegro, is more streamlined and is actively supported. It is primarily intended as a qualitative assessment, although may be used for simple quantitative analysis.

Octave Allegro is an asset focused method. The first step is establishing consistent, qualitative risk measurement criteria specific to the organization's drivers and objectives. After assets have been profiled, threats and impacts are considered in light of real world scenarios to identify risks. These risks are then prioritized according to the risk measurement criteria and planned mitigation.

2.6.3 Control Objectives for Information and Related Technology (COBIT)

COBIT framework is using over fifty sources of good practices from multiple international standards organizations to link IT governance with enterprise governance. The good practices are used for automating IT services as much as possible, without the loss of governance across the business environment. The unification of IT resources occurs by implementing the COBIT process circle, which includes information criteria, planning and organization, acquiring and implementing, delivery and support, monitoring and evaluation, and then returns to the beginning of the cycle.

2.6.4 ISO 27001 Standards

ISO 27001 frameworks help an organization select the proper security measures for their business by utilizing domains of security controls [25]. These domains emphasize the importance of the relationships between informational structures at a generic level. Each of those domains specifies control objectives that give further guidance about how an organization may attempt to implement the framework.

The weaknesses of the ISO 27002 framework are a major lack of guidance as to how to implement the security structures necessary in order to comply with the ISO 27002 standard [25]. This standard takes a wide view of the security standards for an organization and does not drill down into specific actionable requirements necessary to comply with the suggested frameworks. The company or organization implementing these security structures will need a deep understanding of the steps that they will need to take in order to protect their vulnerable information and a broad technical skill set in order to follow the guidelines set forth in the ISO 27002 framework.

2.7 ICSRA Framework Development Procedures

In developing ICSRA framework different researches use their own procedures and steps however, as stated by [26] they share the following steps/ methods of investigation in some order adjustment:

- Inventory and Categorization: Group the information systems, whether internal or external, into categories and differentiate their processes.
- Identify Potential Risks: Look for threats, vulnerabilities and risks that the system might encounter. Natural occurrences such as calamities or power outages should be taken into consideration in addition to malware attacks.
- Implement and Assess: Based on the discussion of potential risks, implement corresponding security controls for data security. Assess and document the findings on how the controls are functioning and contributing to risk reduction.
- Authorize and Monitor: Authorize the operations of the system by determining procedure, the risk to organizational operations and assets, individual strengths and weaknesses, and other factors that will contribute to the welfare of the operations. Monitoring of the security controls is an ongoing process that includes the assessment of the effectiveness of the security controls, documentation of the changes, implementation of the discussed solutions, and presentation of the state of the system to appropriate organizational personnel.

2.8 Summary

As it has been discussed by different researchers even though a lot of frameworks are capable of what the organization needed they have their drawbacks and they need to be urbanized and make it useful for each organization. These frameworks are not specifically designed or developed for banking sector. The researcher’s proposed framework could be a very important input for the banking industry in Ethiopia specifically.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

This chapter presents what research design and method was used to answer the research questions prepared. Review of the research methods: qualitative, quantitative and mixed research methods were followed and choice of the research methods and the reasons for that is declared.

3.1 Components of Research Design and Framework Development Stages

The ICSRA Framework development process has followed the following main research design components and steps which guide the research process. Research design is an outline or guidance of the research.

3.1.1 Main Components

To answer the research questions the following research design techniques are preferred to come up with a fruitful ICSRAF.

I. Literature review: the literature review has been done to the knowledge area of the researcher's proposal.

II. Assessing risk in the banks:-a mixed research methods both Qualitative and Quantitative was applied to assess the current risk and security practices in banks in Ethiopia, problems that impede banks to keep their environment safer, risk identification, risk analysis and risk evaluation. The basis for selecting mixed methods design is to get a better understanding of the problem identified in this research.

III. Propose ICSRAF: - The ICSRA (Information and Cyber Security Risk Assessment) Framework was modeled based on literature review findings and the assessment result of the current practice.

IV. Evaluate the proposed ICSRAF: -The proposed conceptual ICSRA Framework will be evaluated by professionals and will be restructured based on those comments and suggestions.

The overall structure of the thesis would be governed by the following design process flow.

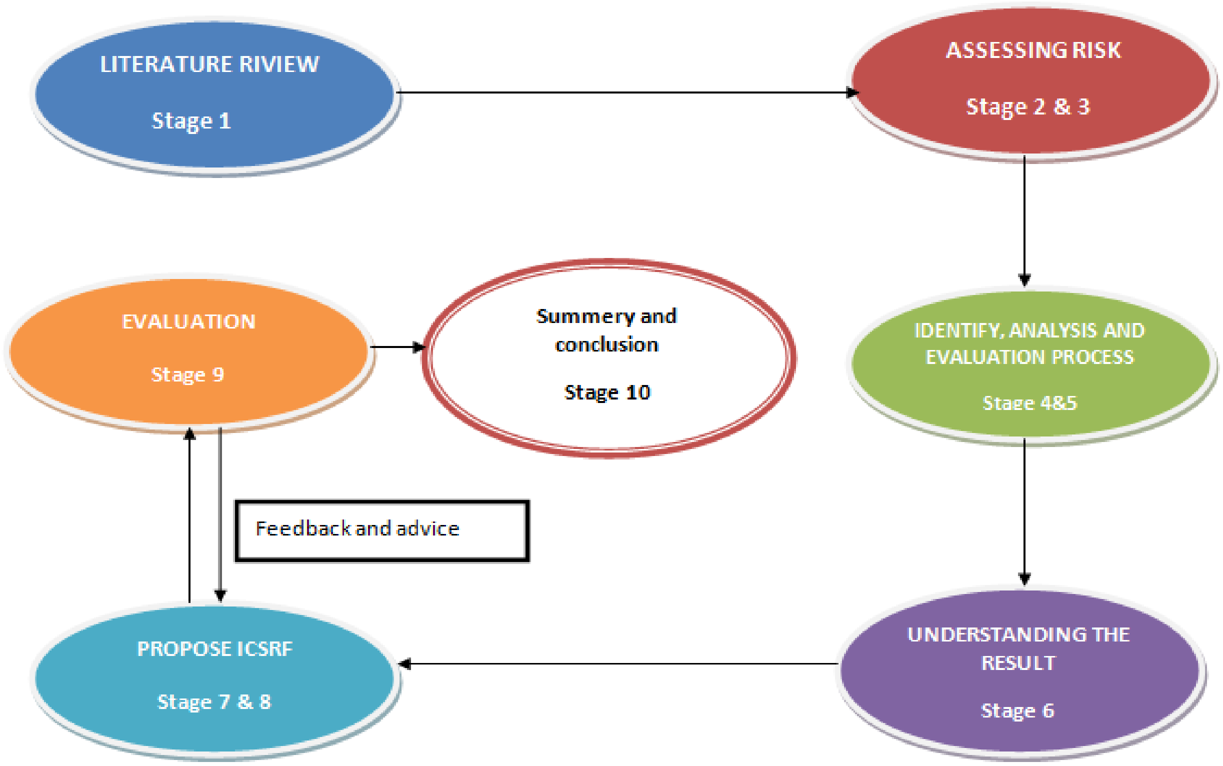


Figure 3.1: Risk Assessment and Framework Development Stages

3.1.2 Framework Development Stages

The above framed risk assessment framework development stages are briefly discussed in such away:-

1. Literature review to grab knowledge about ICSRAF concepts
2. Assessing the current risk in the banking industry by collecting data

   E.g. questionnaire, interview and site survey
3. Analyze the collected data
4. Based on the analyzed data, risk identification and risk analysis would be done
5. Evaluating the risk
6. The results were interpreted within the context of the research framework
7. A conceptual ICSRA Framework was proposed based on the findings of the literature review and assessment results.
8. Evaluate the framework by professionals

9. Fit in feedbacks and advices with the framework for better outcomes
10. Conclusion will be made by summarizing the findings and ICSRA framework and evaluation

3.2 Research Methodology

The study was conducted using survey questionnaire, Site survey and interview as a method of data collection methodology. Mixed methods research refers to the research or lines of inquiry that integrate one or more qualitative and quantitative techniques for data collection and analysis [5]. Qualitative collection methods, including interviews, participant observation, and open ended survey items have great potential for exploring new topics, assisting theory building, and providing context for quantitative data.

3.2.1 Why Mixed Research Method

Using mixed research methodology has advantages such as:-

- Provides strengths it balance the weaknesses of both quantitative and qualitative research.
- Provides a more complete and comprehensive understanding of the research problem than either quantitative or qualitative approaches alone.
- Provides an approach for developing better, more context specific instruments

And has the following drawbacks

- The research design can be very complex.
- Takes much more time and resources to plan and implement this type of research.
- It may be difficult to plan and implement one method by drawing on the findings of another.

This method was selected for this particular study because it was found an appropriate technique for collecting vast information and opinion from respondents. It is also relevant to gather detail description of existing condition and practices of Information and cyber-Security risk management in the bank industry.

3.3 Data Source

The main data sources used in this study are IT top managers, system and network administrators who have decision power related to IT security and those whom their day to day work activity is related with the research premise. This is because; IT departments manage all the information systems functionalities including its security. In addition, secondary sources of data such as relevant best practices, information security risk management policy are used.

3.4 Study Sample

The following banks were incorporated in the study. These are: Commercial Bank of Ethiopia (CBE), Awash Bank (AWB), United Bank S.C (UB), Cooperative bank of Oromia (CBO), Dashen Bank (DB) and Abissynia Bank (AB). These banks are selected by random method.

3.5 Sampling Design and Sampling Techniques

The sampling methods used in the research are clarified as:

3.5.1 Sampling Method

The researcher used random sampling technique; as such it is a Non-probability sample method, for interview and questionnaires purpose in selecting participants from public and private banks. Because of the time limitation, the sampling method used for the interview was purposive sampling technique. In addition, probability sampling was used to select sample banks out of eighteen banks. To select sample banks additional techniques is known as stratified sampling has been used to distinguish the public and private banks and random method to select from sample banks. From the total number of eighteen private and government banks found in Addis Ababa City Administration six banks were selected by lottery method for the study. The following procedure was generally used in the process:

1. The total number of banks in Ethiopia (both private and state owned) regarding was obtained from NBE website.
2. Then stratified sampling method used to distinguish the public and private banks since they are similar.
3. The proportion for selection and distinguishing was determined by computing the ratio of the required sample (n) to the population of the study (N), proportion 6/18=1/3.
4. Apply random method to select sample banks after stratified sampling was done.

5. Purposive sampling technique was applied to select among IT top level security managers, system and network administrators from the sampled banks.
6. Distributing questionnaires and conducting interview with IT security managers, system and network administrators was done with site survey in the six sampled banks.

3.5.2 Scope of the Sample

The targeted population of this research was 6 banks. Thus, six banks were selected by stratified sampling technique.

3.5.3 Sample Size

The sample size of this study is 6 banks and purposive sampling technique was applied to select among IT top level security managers, system and network administrators from these sampled banks.

. This means 30% of the total population ((6/18)*100%).

3.5.4 Data Collection Techniques

The researcher has used four types of tools for data collection purposes, namely: questionnaire, document analysis and interview and site survey. The primary data was collected through questionnaire (structured) interview (unstructured) and site survey.

3.5.4.1 Questionnaire

The question items are open and closed ended questions 10 questionnaires were distributed for one sampled bank and totally 60 questionnaires were distributed for all sampled banks. It was designed based on three categories as operational, business resource, infrastructures and users (Technical and Administrative). The questionnaires were prepared and distributed to IT top managers, system and network administrators of the respective sampled banks. The questionnaire has 49 questions about the business resource, operations, infrastructures and users. The first section dealt with general business resource security management of the respondent bank. The second and third sections inquired about the technical aspect of information and cyber security**.**

3.5.4.2 Interview

Information about interviewees’ experience and knowledge has been collected by the researcher’s prior to conducting the interview 6 interviewees were conducted. They possess the experience and perspective in information security management that this research wishes to understand. Given the security management experience and background of potential interviewees, purposive sampling method seems the most logical choice for data collection.

The main purpose of the interview was to make the questionnaire data more valid and reliable. Because, questionnaire data collected would not be filled as it has been expected. Unlike questionnaire interview can provide a reliable and consistent answers [5].

Because the interviewees are quite busy on their work the researcher has appointed them a week before the interview. It took 30 minutes to discuss the questions with the interviewee. All interviews were conducted face to face, in person, at the interviewees' site of business.

3.5.4.3 Document Analysis

Document analysis on books, articles, conference, best experiences and Internet sources has been made to know the subject area in depth, and assess what techniques other countries and researchers used to develop RAF(Risk Assessment Framework) and how and what measures they took to fight against information and cyber security attacks and threats.

3.5.4.4 Site Survey

Sampled banks; in order to assess the relevance of the instruments designed to collect data and to understand the business process in detail, to recognize what techniques they use to protect their overall system and to visit how users are performing to protect their system from attacks and how they react if something happened. The site survey has been made only for three randomly selected banks from the sampled banks.

3.5.4.5 Procedures

The data gathering tool used in the study was drafted on the basis of the reviewed literature and the planned data to be collected. Prepared questionnaires have been distributed to all respondents. The researcher distributed and collected all questionnaire data. The questioning and answering process has been made in person with interviewees. The researcher has tried to create conducive atmosphere and explain the purpose of the interview to them.

Consequently, necessary information was collected, organized and processed separately for interpreting and summarizing purpose to produce the major findings. Finally, the researcher has proposed information and cyber security risk assessment framework.

3.5.5 Data Analysis and Risk Assessment Methods

3.5.5.1 Data Analysis

After collecting the data, the data has been classified in to groups then it is tabulated. All collected data was organized and processed separately for each item in a way appropriate to answer the questions in the problem statement.

3.5.5.2 Risk Assessment

After analyzing the collected raw data the researcher has organized the categorized and tabulated data for assessment process. The organized data used as an input for risk assessment process which would be inserted for the selected risk assessment tool. For the purpose of risk assessment RM studio has been selected based on the analysis and discussion made in Table 2.1. The risk assessment process has five stages in RM studio assessment procedure they are:

1. Identify business entities: business entities are the type of business that is going to be assessed.
2. Identify assets: identifying which type of information assets are going to be assessed.
3. Identify threats: the system automatically generates possible threats for corresponding assets.
4. Assess the risk: prioritize each degree of threat and
5. Report generations: finally it generates final report.

CHAPTER FOUR

FINDINGS INTERPRETATION AND IMPLICATIONS

In this section findings of the study and its interpretations are presented under each question items whereas implications are stated at the end of each security category.

4.1 Respondent Information

The respondents of the research include IT staffs who are engaged in managerial position and IT officers who are working in IT security office including system administrators and network administrators.

4.2 Questionnaires

After preparing a questionnaire accepting recommendations from my adviser, the questionnaires were personally distributed to the sampled banks. And then the researcher has collected the filled questionnaires. The questionnaires are attached as Appendix A at the end of this document.

St. Mary's University has prepared a cooperative letter for these banks and it makes the job easier and acceptable by the banks. And it used as a guarantee that the information provided is to be used only for academic research purposes.

The data collection took almost a month to get all papers which are distributed to be filled by the respondents.

4.3 Response

The questionnaire which has been distributed to the sampled banks has been collected properly. The response rate is 100%.

$$\frac{\boldsymbol{Number\ of\ completed\ questionnairex=60}}{\boldsymbol{Number\ of\ distributed\ questions=\ 60}} = \mathbf{1\ \boldsymbol{X}\ 100 =\ 100\%}\ \dots .\ \dots\dots\dots\dots\dots\dots.. \qquad \text{Equation 4.3-1}$$

This number shows as the response rate is high and it is possible to continue on analysis of the collected data.

4.4 Findings

In this section, the results from data analysis are presented addressing the main components of information and cyber security risk management. The data analysis result is demonstrated.

From the questionnaire and site survey collected data the researcher have organized the data to identify the information assets of the surveyed banks.

4.5 Interview Analysis of Opinions

The analysis of qualitative data is done using spectator idea. Interview findings are described in terms of words:

The aim of this analysis is to examine the different IT security managers' views and ideas regard to the management of information security the interviewees hold, as well as to arrive at strong descriptions of these views. The organization of this section is presented as follows: First, each interview question is presented along with a strong text that describes each interviewee's view. Then, a final synthesis has been made that incorporated these views under each question.

4.5.1 What kind of IT risk management methodology or standard you have used? if not does you bank developed any RA/RM framework?

Bank 01 stated that for a long period of time there was no formally and compressively developed RA/RM rather there were a uneven policies and procedures that the bank has employed. bank 01 has also stated that mostly in the banking industry even though risk management is a vital focus area most of the banks don't have a dedicated office which can handle risk management issues.

Bank 02` explained that there is no formal and compressive ICSRA methodology rather there are informal or unwritten standards they implement to assess the risk. However, banks use risk management techniques which are not formally and designed for the business sector, As a result, the top management has established risk management team.

According to bank 03 there is no comprehensive IT security policy in the bank. However, currently there is an initiation from IT department to develop and implement risk management which is conformity with the regulatory requirements of National bank of Ethiopia.

bank 04 noted that there is no formally developed RA/RM method rather there is non-formalized policies and procedures that the bank applied to protect its information asset based on pre-attack protection. As bank 04 explained, Lack of information security understanding by top management, lack of motivations even within IT department, lack of budget due to less attention of top management, and lack of experts are some of the challenges.

Bank 05 stated that there is no formal developed RA/RM methods rather there is non-formalized and fragmented policies and procedures that the bank applied to assess its risks. The bank doesn't develop any kind of risk management methodologies because there is a lack of understanding about information security management on the top management.

Bank 06 has stated there is a risk management office in the bank which has the responsibility of taking care of risk issues on the banks information security environment. But RA/RM process is held in an informal way.

4.5.2 Does your organization implement a risk assessment?

Bank 01 has stated that since his joining of the bank he doesn't have seen any risk assessment process but the interviewee has explained risk management should be considered as a primary job for the information security management system.

Banks 02 and 03 have explained there is a risk assessment team in the bank information security department and the team has assessed the risk informally (without any standards).

Banks 04 and 05 have stated that there is no motivation to perform a risk assessment process in the bank. Because they claimed that the top level managers give a lesser attention for information security management systems. Bank 06 has stated there is no formal risk assessment process in the bank.

4.5.3 Does your organization ever faced with any kind of external or internal attack?

Bank 01 has stated that attack would came in different and in indistinguishable ways because banking industries are mostly targeted by hackers for theft purpose. As bank 01 described they hadn't faced a significant attack since his joined of the bank. But he critically emphasized that there should be a mechanism to assess risk and if it happen there should be a risk management methods in place. Banks 02, 03, 04 and 05 has affirmed that they haven't seen any attack which make their banks lose its many or reputability in the market.

Bank 06 has confirmed that there were some cyber-attacks which make the banks lose money and reputation which they cannot measure it is in terms of monetary value. As bank 06 interviewee described after the attack happened the bank has taken measures to protect its network by re-designing its information security management systems.

4.5.4 What do you suggest for banks to deploy a risk management process?

According to bank 01 unless otherwise the bank knows its assets and the level of protection needed security may not be assured. Thus the information asset classification scheme should be based on potential financial consequences of a security breach. Unfortunately, the bank does not have IT risk management methodology. However, bank 01 Interviewee suggests that one should approach IT risk management by following these steps strictly:

- Identifying products/services that generate material revenue streams
- Identify threats
- Evaluating current security in the IT systems
- Deciding on the needed security level based on the financial risk exposure; and
- Implementing the security level as technical controls.

Bank 02 thought that to achieve Risk Management objectives, the IT department of the bank must work closely with business departments or operations to create effective risk analysis and protection mechanisms.

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

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

Bank 05 Interviewee has emphasized that banks should follow ISO standards to assess their risk by their domain experts.

Bank 06 interviewee observed that there is no predefined IT risk management methodology. Risk management is handled by business risk and compliance department of the bank. In essence, interviewee 06 argues that information security should be based on business processes, economics, and management of risks. A holistic approach in risk analysis process is essential. Thus, first the bank's asset that support business process must be identified, risk assessment be performed, risks must be prioritized based on their severity level, appropriate (economical) controls must be selected and implemented.

4.5.5 What are the disadvantages and strengths of the model that you have employed for Risk Assessment?

Because there is no standardized risk assessment model developed specifically for banks it is difficult to tell about its strengths and weakness. Banks 2, 3, 4, 5 and 6 Interviewees can’t describe the strength or weakness of the model because it is not clearly communicated with them.

All banks interviewees have agreed on the necessity of a business oriented risk assessment framework development. All banks in Ethiopia doesn’t develop even they don’t implement risk management model which are developed by external organizations.

In the surveyed banks it is observed that security issues are not considered as primary issues. The interviewees stated that their banks use unformulated risk assessment methods. In some banks even though there information security departments their job is only to monitor information security flaws. They don’t have a backup plans to countermeasure attacks from inside or outside.

The banks interviewee’s response in general has coded in three nodes which are selected to measure the frequency of words during interview and the degree of the word with the questions.

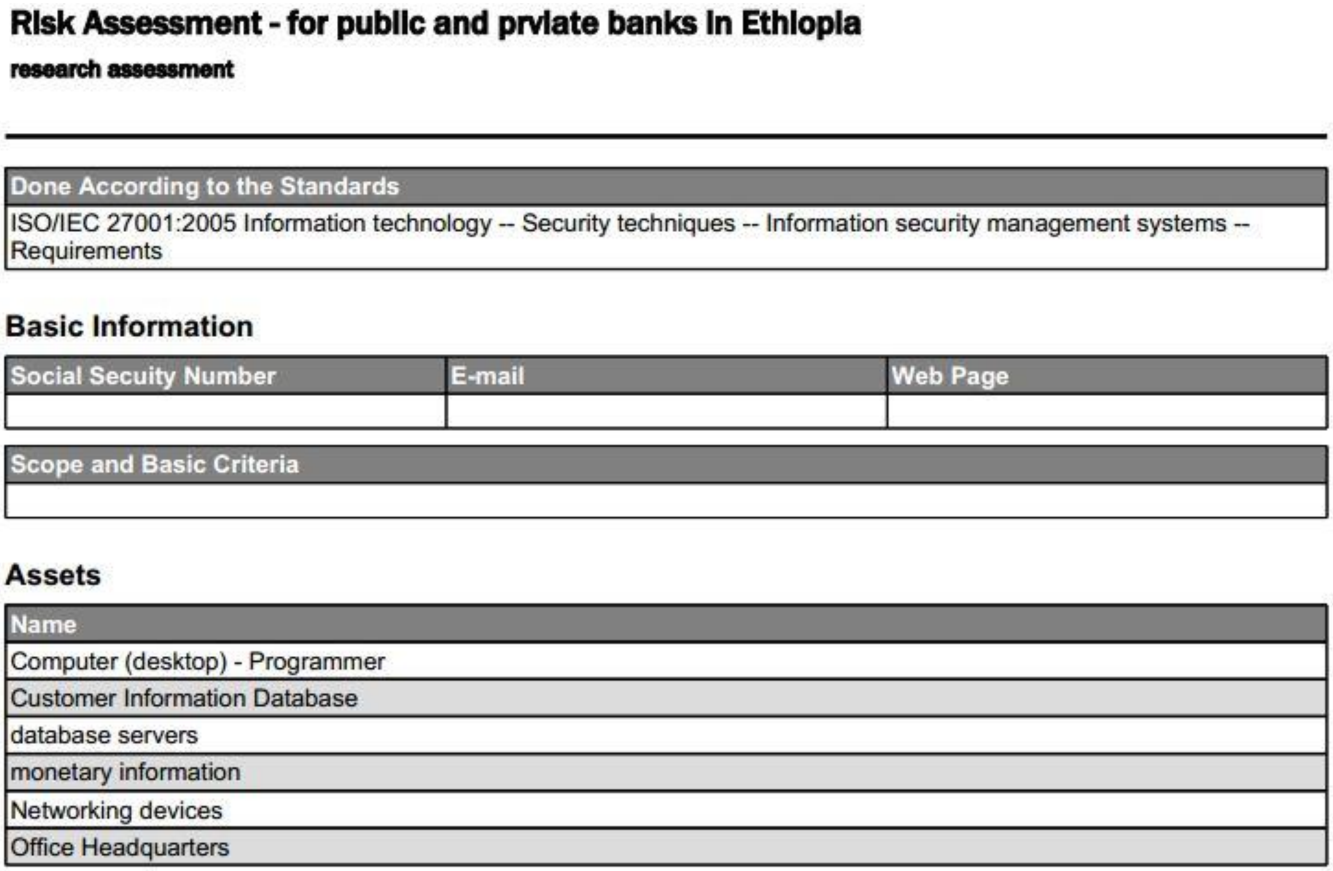
4.6 Observation analysis

The researcher observed that in all Ethiopian state and private banks there is no formal information and cyber security risk assessment methods or frameworks. As it has been identified in almost all banks the researcher observed a negligence of protecting information or cyber assets.

During data collection (observation and questionnaire) the researcher identified assets which and evaluate their risk and rate them accordingly.

4.7 Asset Identification

This section demonstrates the information assets which are identified through site survey and questionnaire data collection process.



Risk Assessment - for public and prviate banks in Ethiopia

research assessment

Done According to the Standards
ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements

Basic Information

Social Secuity Number	E-mail	Web Page

Scope and Basic Criteria

Assets

Name
Computer (desktop) - Programmer
Customer Information Database
database servers
monetary information
Networking devices
Office Headquarters

Figure 4.1: Asset Identification

4.8 Identify Realistic Threats

The goal of this step is to identify the potential threat sources and compile a threat statement listing potential threat-sources that are applicable to the covered entity and its operating environment. The listing of threat sources has included realistic and probable human and natural incidents that can have a negative impact on the specified asset. RM studio identified all possible threats for the corresponding assets. The researcher altered the threats during observation.

Name of the Threat	Name of the threat
Natural Disaster – earthquake	Degradation of availability
Malicious attack – electromagnetic radiation(act of war)	Inadvertent manipulation of data
Staff shortages	Malicious attack – manipulation of data or software
User errors	Negligent deletion of data
Password exposure	Cross talk
Exposure of documents / data	Degradation of paper documents
Careless communication of information to unauthorized recipient	Back-ups unavailable
Duress to staff	Failure of backed up data
Entrapment / blackmail of staff	Corruption of data
Failure to use software patches to cure known security weaknesses	Denial of service
Links remaining active on completion of communications through ISDN	Theft / loss of tell working equipment / data
Uncontrolled copying of documents	Manipulation of teleporting equipment by family/ visitor
Malicious attack –intention of theft	Failure to back up data/ documents
Uncontrolled disposal of documents	Malicious attack – manipulation of IT equipment
Failure to receive information	Failure to change passwords regularly
Uncontrolled use of resources	Failure to use security measures provided
Uncontrolled use of communications links	Abuse of security measures – 'tailgating', misuse of access
Loss of confidentiality	Unauthorized use of data stored on PABX (Private Automatic Branch
Loss of availability to authorized users	Misuse of email services
Infringement of copyright law	Adverse publicity from unguarded media 'interview'
Degradation in response time	Extended response time through different time zone / working hours
Failure of gas supply	Breach of legislation
Failure / degradation of IT equipment	Exploitation of known weakness
Failure / degradation of communications system	Malicious attack –access to site services
Natural Disaster –lightning	Verification difficult / impossible
Failure of long range communications dependent on P.T.O.(Public	Validation difficult / impossible
Failure of equipment / system due to date format ambiguity	Poor control of coding methodology
Death / injury of personnel	Inadequate records of changes / modifications
Inadequate IT / communications capacity	Opportunity for 'back-door 'access into Information System
Illegal use of software	Unexpected performance
Use of software by unauthorized users	Users not known
Use of software in an unauthorized way	Lack of complete testing
Unauthorized use of storage media	Industrial action
Masquerading of user identity	Swine flu –A(H1N1)
Network access by unauthorized users	Unauthorized access to site
Malicious attack – explosives	Unauthorized access to building
Use of network facilities in an unauthorized way	Unauthorized access to room
Communications infiltration	Accidental damage –aircraft
Misrouting of communications	Natural Disaster –hurricane
Connection of unauthorized equipment	Accidental damage –vehicular collision
Accidental damage – strong magnetic fields	Accidental damage – [from] Building material
Accidental damage – during building construction / maintenance	Accidental damage – fire
Natural Disaster – flooding	Accidental damage – water / soiling

Figure 4.2: Threat Identification

4.9 Relating Threats to Vulnerabilities

This relates the threats identified and vulnurablity of the assets to that threat. Mostly relating thereat with vulnurablity is a major task and requires a serious attention. Most of these activies has been done using RM srudio which can help the result to be more scientific for decision.The definition of asset and threat properties is attached in Appendix C.

Asset	**Description**
Computer (desktop) – Programmer	Computer for programmer and users

Threat Name	**Impact of Threat**	**Probability of Threat**	**Vulnerability of Asset**
Abuse of administrator rights	Very High	High	High
Abuse of user rights	Very High	High	High
Boot viruses	Very High	low	low
Deliberate overloading of service	Very High	High	High
Inappropriate use of communications equipment	Very High	High	High
Inappropriate use of storage media	Very High	High	High
IP spoofing	Very High	low	High
Malicious attack – chemical	Very High	High	High
Malicious attack - incendiary device	Very High	High	High
Malicious attack	Very High	low	High
Misuse of resources	Very High	High	High
Social Engineering	Very High	High	High
Theft of consumables	Very High	low	High
Theft of data / documents	Very High	High	High
Theft of equipment	Very High	High	High
Theft of mobile equipment	Very High	High	High
Theft of software	Very High	low	low
Traffic analysis	Very High	low	low
Trojan code	Very High	low	Medium
Unauthorized use of IT systems	Very High	Medium	High
Unauthorized viewing, copying, removal of archived documents	Very High	Medium	low
Uncontrolled downloading of software	Very High	High	High

Figure 4.3: Computer Desktop

As shown in the above Figure4.3, the surveyed banks have been examined by the parameters which are urbanized by ISO/IEC 27001:2005 standards. As the survey data implies banks regarding personnel including IT specialsts and end users who perform a day to day activity on the information process the impact of the threat is VERY HIGH, the probablity of theese threats is HIGH and the vulnereblity of these assets would be HIGH.

Asset	Description
Customer Information Database	Database which store all of the customer information.

Threat Name	Impact of Threat	Probability of Threat	Vulnerability of Asset
Access to systems / documents by maintenance, service and cleaning staff	Very High	Medium	Low
Accidental damage - breakage by personnel or equipment	Very High	Medium	Medium
Back-ups unavailable	Very High	Medium	Medium
Communications infiltration	Very High	Medium	Low
Corruption of data	Very High	Medium	Medium
Degradation in response time	Very High	Medium	Medium
Degradation of availability	Very High	Medium	Medium
Entrapment / blackmail of staff	Very High	Medium	Medium
Failure / degradation of IT equipment	Very High	Medium	Medium
Failure of backed up data	Very High	Medium	Medium
Failure of equipment / system due to date format ambiguity	Very High	Medium	Medium
Failure of long range communications dependent on P.T.O.(Public Telecommunications Operator)	Very High	Medium	Medium
Failure to back up data / documents	Very High	Medium	Medium
Failure to receive information	Very High	Medium	Medium
Failure to use security measures provided	Very High	Medium	Medium
Inadequate IT / communications capacity	Very High	Medium	Low
Inadvertent manipulation of data	Very High	Medium	Medium
Inappropriate use of storage media	Very High	Medium	Low
Malicious attack - electromagnetic radiation	Very High	Medium	Medium
Malicious attack - intention of theft	Very High	Medium	Medium
Malicious attack - manipulation of IT equipment	Very High	Medium	Medium
Malicious attack	Very High	Medium	Low
Malicious software (e.g. viruses)	Very High	Medium	Low
Misuse of email services	Very High	Medium	Medium

Figure 4.4: Customer Information Database

As the survey data implies banks regarding database which is a center of customer information, the impact of the threat is VERY HIGH, the probablity of theese threats is MEDIUM and the vulnereblity of these asset on manipulation of IT equipments, failure to back up data is MEDIUM but malicious software malicious attack is LOW.

Asset	Description
database servers	Database servers which contain other information

Threat Name	Impact of	Probability of	Vulnerability of
Abuse of administrator rights	Immense	Medium	Low
Abuse of user rights	Very High	Medium	High
Breach of legislation	Very High	Low	Low
Degradation in response time	Very High	Low	Low
Degradation of availability	Very High	Low	Low
Deliberate overloading of service	Very High	Medium	Low
Failure / degradation of IT equipment	Very High	Low	Low
Failure of backup power supply (UPS)	Very High	High	Low
Failure of equipment / system due to date format ambiguity	Medium	Medium	Low
Failure of long range communications dependent on P.T.O.(Public Telecommunications Operator)	Very High	Low	Low
Failure of power supply	Very High	Low	Low
Failure of water supply	Very High	Low	Low
Inadequate IT / communications capacity	Very High	Low	Low
Inadequate records of changes / modifications	Very High	Medium	High
Lack of audit trails	Very High	Low	Low
Maintenance error	High	Medium	High
Malicious attack - manipulation of IT equipment	Very High	Low	Low
Misuse of remote access ports for management / diagnostics	Very High	Low	Low

Figure 4.5: Database Server

As the survey data implies banks regarding database servers. the impact of the threat is VERY HIGH, the probablity of theese threats is MEDIUM but these servers have been kept in a critical security conditions.

The probablity of threats is LOW and the vulnereblity of this asset is mostly LOW but maintenance error, inadequate records of changes / modifications has HIGH.

Asset	Description
monetary information	Information which contains different transaction

Threat Name	Impact of	Probability of	Vulnerability of Asset
Access to systems / documents by maintenance, service and cleaning staff	High	High	Medium
Accidental damage - breakage by personnel or equipment	High	Medium	Medium
Back-ups unavailable	High	Medium	Low
Communications infiltration	Medium	Medium	Medium
Failure of equipment / system due to date format ambiguity	High	Medium	Low
Failure of long range communications dependent on P.T.O.(Public Telecommunications Operator)	High	Medium	Low
Failure to back up data / documents	High	Medium	Low
Failure to receive information	High	Medium	Low
Failure to use security measures provided	High	High	Medium
Inadequate IT / communications capacity	Medium	Medium	Low
Inadvertent manipulation of data	Very High	Low	Low
Inappropriate use of storage media	High	Medium	Low
Malicious attack - intention of theft	Immense	High	Medium
Malicious attack - manipulation of IT equipment	High	High	Low
Malicious software (e.g. viruses)	High	Low	Medium
Misuse of email services	Low	Medium	Medium
Operational staff error	Very High	Low	Low
Password exposure	Very High	Medium	Low
Social Engineering	Very High	Medium	Medium

Figure 4.6: Monetary Information

The data collected concerning monetary information is, its impact of the threats is VERY HIGH, the probablity of theese threats is MEDIUM but Voltage spikes / surges / fluctuations, Unlicensed use of software and Failure to use security measures provided have a HIGH probability rate. Unlike the other two parameters regarding vulnerability of asset for monetary information is LOW and MEDIUM because sampled banks give priority to protect their monetary information.

Asset	Description
Networking devices	Networking infrastructure

Threat Name	Impact of	Probability of	Vulnerability of Asset
Abuse of administrator rights	Very High	Medium	Low
Abuse of security measures – 'tailgating', misuse of access tokens, etc	High	Medium	Low
Abuse of user rights	Very High	Medium	Low
Accidental damage - [from] Building material	High	Medium	Low
Accidental damage - breakage by personnel or equipment	High	Medium	Low
Accidental damage – fire	High	Medium	Low
Accidental damage - vehicular collision	High	Medium	Low
Analysis of message flow	Very High	Medium	Low
Breach of legislation	High	Medium	Low
Connection of unauthorized equipment	Very High	Medium	Low
Cross talk	High	Medium	Low
Degradation in response time	High	Medium	Low
Degradation of availability	High	Medium	Low
Deliberate overloading of service	Very High	Medium	Low

Figure 4.7: Networking Devices

The above figure shows us the surveyed banks used networking and communiation devices as a basic resource to trnsmit and exchange data. Though, the threats imapact on these devices are VERY HIGH, but the probablity of these threats are MEDIUM which implies that there would be an attack at any time. But the vulnerablity of these assests for attack is LOW.

Asset	Description
Office Headquarters	Physical office building for the bank

Threat Name	Impact of Threat	Probability of Threat	Vulnerability of Asset
Abuse of security measures – 'tailgating', misuse of access tokens, etc	Very High	Medium	Low
Accidental damage - [from] Building material	Very High	Low	Low
Accidental damage - air conditioning failure	Low	Medium	Medium
Accidental damage – aircraft	High	Low	Low
Accidental damage - breakage by personnel or equipment	Medium	Low	Low
Accidental damage - chemical pollution	Low	Low	Low
Accidental damage - during building construction / maintenance	Medium	Low	Low
Accidental damage - extremes of temperature / humidity	Medium	Low	Medium
Accidental damage – fire	Very High	Medium	Low
Accidental damage - strong magnetic fields	Medium	Low	Low
Accidental damage - vehicular collision	High	Low	Low
Accidental damage - water / soiling	High	Low	Low
Damage - animal / insect / bacteriological	Medium	High	Medium
Failure of gas supply	Medium	Low	Low
Failure of power supply	High	Medium	Low
Failure of water supply	Low	Low	Low
Failure to use security measures provided	High	High	High
Inadequate records of changes / modifications	Very High	Medium	Low
Maintenance error	High	Medium	Low
Malicious attack - access to site services	Very High	Medium	Low
Malicious attack – chemical	High	Medium	Low
Malicious attack – explosives	High	Low	Medium

Figure 4.8: Office Headquarters (Datacenter)

As depicted in the above Figure in surveyed datacenters and buildings, the threats which could occur has a VERY HIGH, impacts on the operation and the probability of these threats are mostly MEDIUM, but malicious attacks, damage - animal / insect / bacteriological and Failure to use security measures provided are HIGH probability, Regarding the vulnerability of the asset to attack is LOW. In some cases such as malicious attack - intention of theft and failure to use security measures provided is HIGH.

4.10 Likelihood of the Threat (Probability of Threat)

A likelihood assessment estimates the probability of a threat occurring. It is necessary to determine the circumstances that will affect the likelihood of the risk occurring. The likelihood can be expressed in terms of the frequency of occurrence, as it is stated in the above Figures such probability of the threats has been evaluated by "HIGH, MEDIUM, LOW, VERY HIGH and EXTREME. The greater likelihood of a threat occurring the higher the risk is. It can be difficult to reasonably quantify likelihood for many parameters; therefore, relative likelihood can be employed as a ranking. An illustration of this would be the relative likelihood in a geographical area of an earthquake, a hurricane or a tornado, ranked in low rated of likelihood.

4.11 Risk Assessment Results

Risk assessment is prioritizing of risks based or probability and impact of an event. So it can be concluded that the threats which their impact is rated HIGH, VERY HIGH or EXTEREME and which their probability is rated HIGH, VERYHIGH or EXTEREME and their vulnerability is rated HIGH, VERY HIGH or EXTEREME should be given a serious attention and risk mitigation process should be initiated.

4.12 Security Controls

Controls are all those countermeasures or safeguards that are put in place in a bank and that make up the information security. Classified under these categories are:

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

- Logical and Administrative Controls Access
- Rights Administration · Authentication
- Acceptable Use Policy
- Network Access
- Operating System Access

- Application Access · Remote Access
- Risk assessment and management process
- Antivirus, Code Blocking, Content Management, Email scanners
- Firewall, gateway rules and/or filters
- Policies and procedures

Physical Security:

- physical security zones, i.e., data center vs. branches
- Controls for environmental hazards, such as fire, flooding (halo gas, smoke alarms, raised flooring, heat sensors, etc; ·
- Power outages and fluctuations · Alarms, surveillance cameras, synchronized lighting, and other intruder detection devices
- Backup communications · Vaults, locked cabinets, equipment and paper storage, media storage
- Locks or other devices for PC, laptops, hand-held devices, etc.
- Protected cabling, routing of cabling wire rooms locks, Infrared or wireless equipment, frequency emissions both wireless and unintentional emissions from unshielded equipment
- Badges and physical ID control

Encryption:

- transmission
- Storage
- Key Management
  - ✓ Uses by Type
  - ✓ Hashes: verify file and message integrity and passwords from disclosure
  - ✓ Symmetric keys: used with asymmetric keys, which perform key exchange to establish encrypted session with symmetric key
  - ✓ Asymmetric or Public keys, key exchange

Logging and Data Collection:

- Identify components to be logged (i.e., firewall events, network traffic, intrusion detection system events, application and operating systems, etc.)
- Specify information to be logged
- Protect logged data from destruction or manipulation
- Review and analysis of logs, escalation procedures and required responses and reporting
- Type of Intrusion detection system to use -- heuristic or signature – based on objectives ·
- Proper placement of Intrusion detection system ·
- Apply various countermeasures on typical methods used to defeat the IDS or to generate false positives or false negatives;

4.13 Summary

The researcher finally found out that the results which it has been shown above and literature reviews was used as a startup to develop the assessment framework. After completing risk assessment it is possibly simple to tell the extent to which information and cyber security threats might cause a loss or failure in the financial organizations in Ethiopia.

CHAPTER FIVE

THE PROPOSED ICSRA FRAMEWORK

A risk assessment framework (RAF) is a system for prioritizing and sharing information about the security risks posed to any organization using information technology as a business process backbone. The information should be presented in a way that both non-technical and technical personnel in which group can understand. The view on the RAF provides assistance to organizations in identifying and locating both low and high-risk areas in the system that may be vulnerable to abuses or attacks.

The data that RAFs provide is beneficial for addressing potential threats and planning costs and budgets. Many RAFs are already accepted as standards in several industries. A few examples include the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) from the Computer Emergency Readiness Team, the Control Objectives for Information and Related Technology (COBIT) from the Information Systems Audit and Control Association, and the Risk Management Guide for Information Technology Systems from the National Institute of Standards and ISO standards..

Banks in Ethiopia have different goals, strategies, organizational cultures and structures. Consequently, the ideal management system and the way to achieve it will differ among banks. Thus, this study proposed a framework that can be used to assess the risks related to information and cyber security.

The proposed framework has ten major components: understanding the scope of the system, asset characterization, and parameter identification, threat identification, relating threats with asses, vulnerability analysis, risk prioritization, risk analysis and evaluation, risk communication, documentation and mitigation methodology.

The framework was developed by review of literature and related works which has been done by different researchers. And data collection methods (site survey, company’s best practice, questionnaire and interview) facilitated the framework process to be more inclusive and more business oriented.

5.1 Objectives of the Proposed ICSRA Framework

- To provide an ICSRA framework to support banks security risk management processes.
- To enable a strategic approach to information and cyber security management by providing simplified and holistic solutions for decision making and consideration.

5.2 Major Components of the Proposed ICSRA Framework

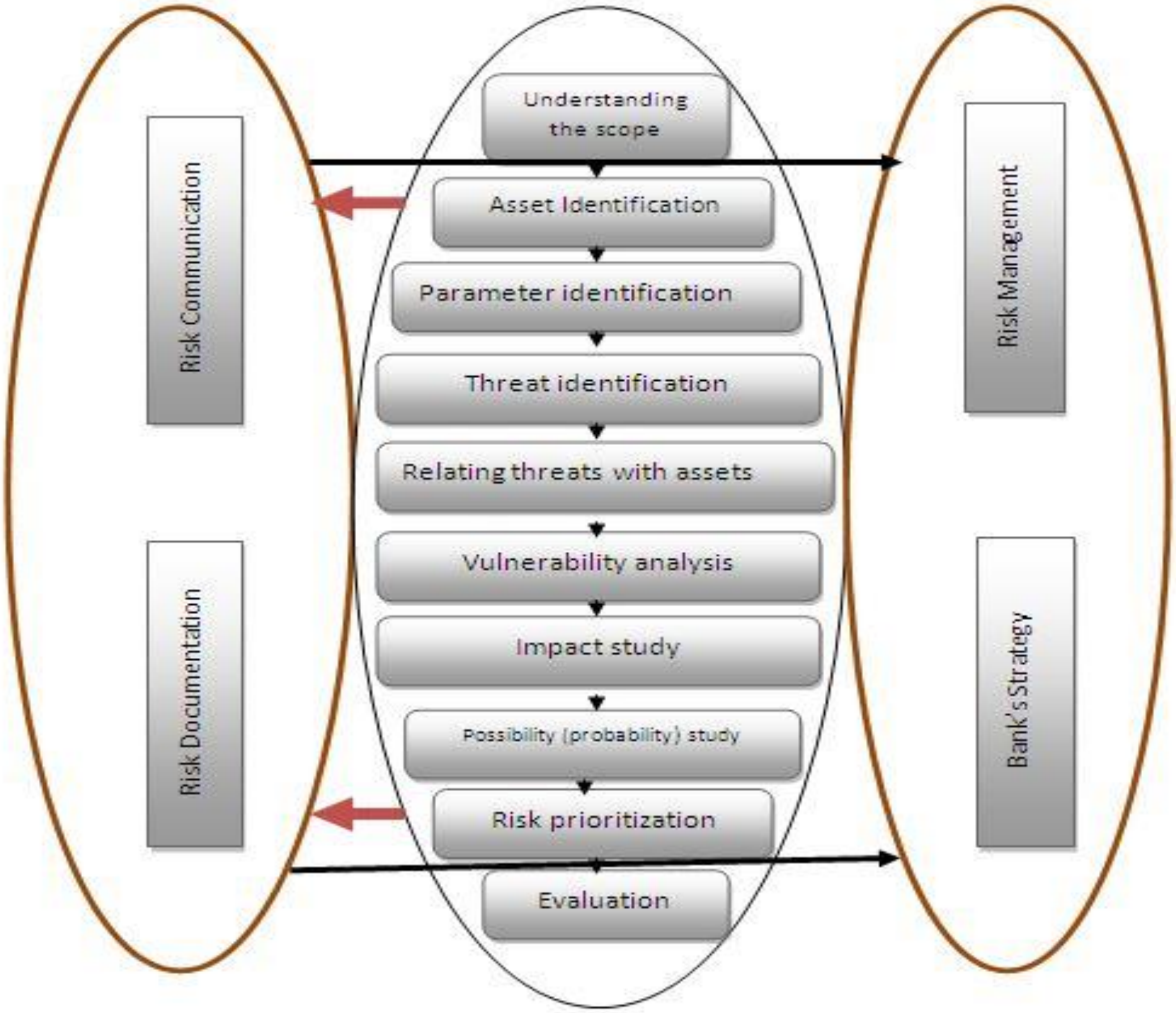


Figure 5.1: The Proposed ICSRA Framework

Internal Components

1. **Understanding the scope of the system:** understand the range of the system that should be covered in the assessment process such as:-identifying stockholders and their relationship (entity relationship model)
2. **Asset identification and characterization:** characterize the assets of the organization such as:-hardware, software, service.
3. **Parameter identification:** identify the measurement parameter which can be used as tools for the purpose of characterization. Such as vulnerability, confidentiality, value, availability and so on.
4. **Threat identification:** investigates the assets' possible threats.

5. **Relating threats with assets:** asset threat relationship and mapping.
6. **Vulnerability analysis:** analyzes how susceptible is the asset to that threat
7. **Impact study:** identify the impact of the threat against its assets.
8. **Possibility (probability) study:** determine the probability of occurrence of threats
9. **Risk prioritization:** assess the risk by ascending or descending order
10. **Evaluation:** evaluating the results

External Components

11. **Risk communication:** exchange of real-time information, advice and opinions between experts and stockholders.
12. **Risk documentation-** documenting the findings during assessment.

The six surveyed banks' interviewees (Section 4.7) explanation indicates that there is no a predefined risk assessment or risk management model. Currently, all surveyed banks employed the combination of general knowledge and experience of experts, and adopting federal agencies recommendations. In addition, available standards lack clear steps in risk management process, thus, to come up with this framework is a comprehensive and easier tool for all of them.

5.3 Design of ISCRA Framework

The proposed framework could be a starting point for banking sector to manage risk in developing and implementing RA/RM to protect banking information assets from the threats recognized in literature reviews, interview and questionnaires of the study. However, the suggested framework is still a general approach to information security and cyber security management program, but all the component parts of this framework need to be addressed to have full control of information and cyber security resources and assets. This framework is an integration of available standard components discussed and some of the features derived from literature review.

Internal components: are components of the proposed framework which are composed in to the risk assessment process. These processes are done by a risk assessment team.

5.3.1 Understanding the Scope of the System

Understanding the scope of the system is a major task in the proposed framework. Banks have different stakeholders which are considered as an entity. Consequently entity relationship is employed to identify and represent inter entities (organizations which have interaction with a bank) and intra entities (departments or processes which have interaction with RA/RM process within a bank). In addition, this ERM is used to define information flow (in one or two way communication) between business entities [25].

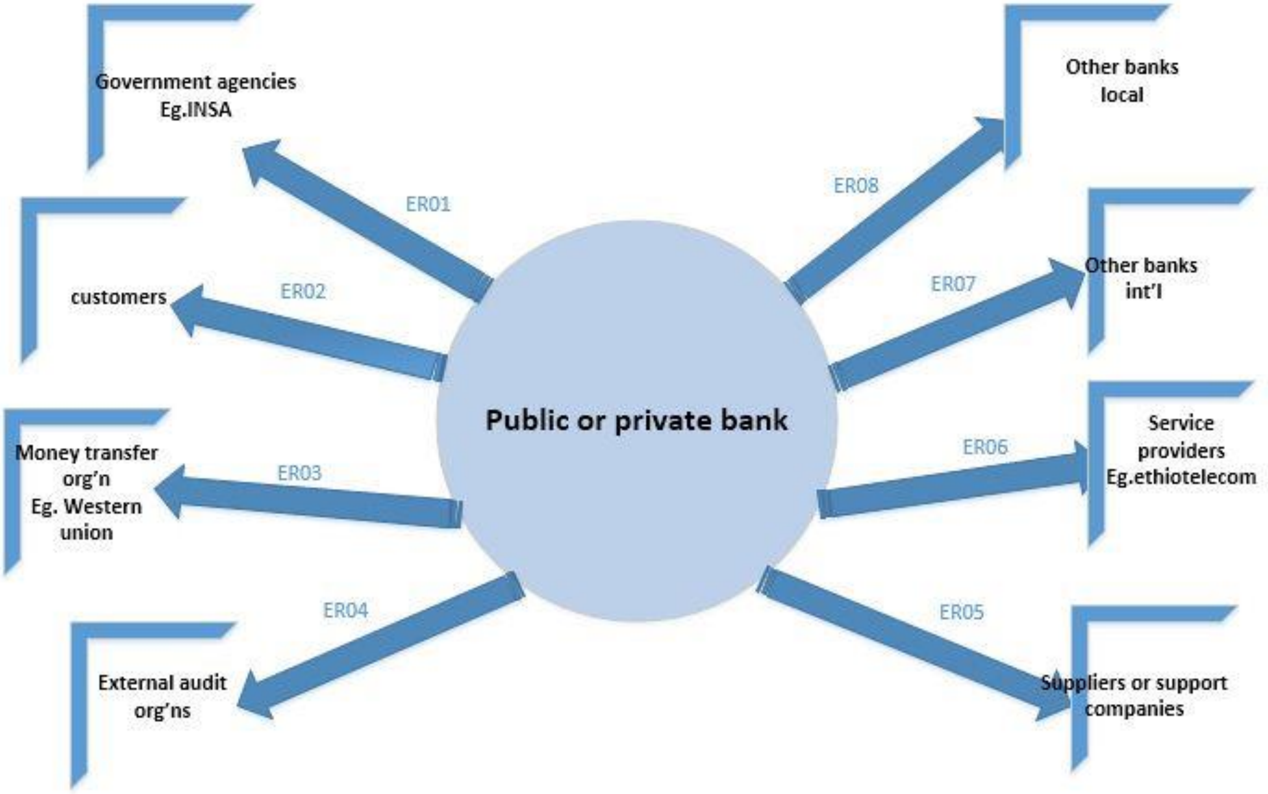


Figure 5.2: Entity Relationship

5.3.1.1 Description of Entity Relationship

Entity correlation diagram shows a brief relationship between entities. It is also used to identify a type of information assets, resources required for business process and level of interaction through the communication channel [5]. Each entities and relationships will be discussed as follows:-

i. **Government agencies**: - government agencies such as INSA and other agencies which are directly related with banking business process. INSA has a direct influence in the banking information security process because banks use INSA recommended information security policies.

ii. **Customers*:*** a customer is a person or organization that is accessed one or more of the services provided by the bank.

iii. **Money transferring organizations*:-***financial institutions which has a business objective and agreement with the bank. E.g. Western Union, Dahabshil, e.t.c

iv. **External audit*: -***an organization which is authorized by the government to carry out an analysis and inspection of financial operation for the banks independently.

v. **Suppliers and support companies*:-***companies which supply service and products for the banks inquiry and also support companies like oracle, Microsoft, Cisco, IBM, e.t.c

vi. **Service providers*:-*** organizations which provides their service for the banks e.g. Ethio telecom, EEPU(Ethiopian Electric Power Utility) and others

vii. **Other international banks*: -*** banks which are located abroad and provide international banking service collaboratively operational with Ethiopian banks.

viii. **Other local banks*: -*** A type of finical service providers which has a business objective and agreement with Ethiopian Bank. For example, the relation between CBE with NBE(National Bank of Ethiopia).

5.3.1.1.1 Stakeholders business correlation with public or government banks

- ER01:- business correlation between government agencies and Ethiopian public or private bank
- ER02:- business correlation between Customers and Ethiopian public or private bank
- ER03:- business correlation between money transfer organizations and Ethiopian public or private bank
- ER04:- business correlation between external audit and Ethiopian public or private bank
- ER05:- business correlation between suppliers and support companies and Ethiopian public or private bank
- ER06:- business correlation between service providers and Ethiopian public or private bank
- ER07:- business correlation between other international banks and Ethiopian public or private bank
- ER08:- business correlation between other local banks and Ethiopian public or private bank

5.3.1.2 Intra-bank Entity Correlation

In the bank there are different departments which are responsible for their corresponding function. These departments are working together to achieve a common goal. Intra banks entity correlation is should be done by considering each process or department and branch as one entity.

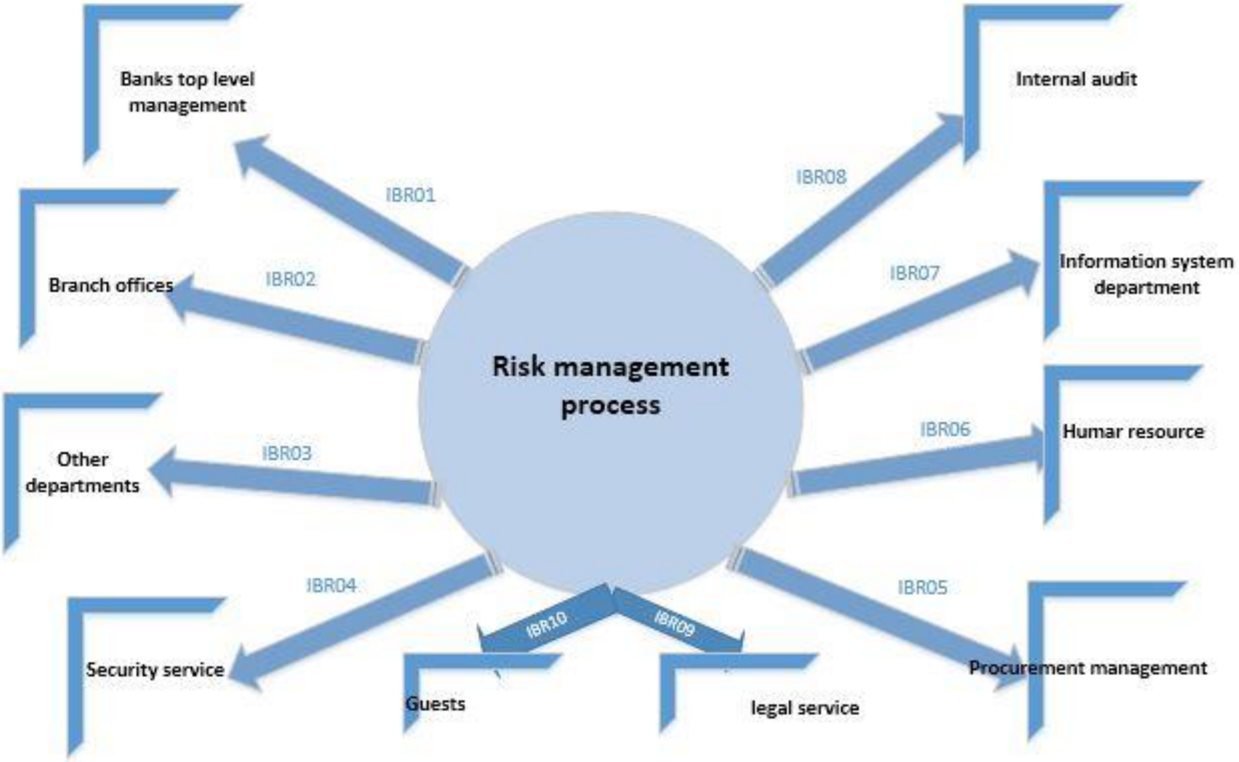


Figure 5.3: Intra-bank Entity Correlation

5.3.1.2.1 Description on Intra-bank correlation

i. **Banks top level managements*:* -**the banks top level management plays a great role in the risk management process because top level managements are policymakers.

ii. **Branch offices:** - the banks local office which gives a banking service.

iii. **Other departments**:- business departments which work in the back or front office

iv. **Security services**:- departments which give a security and cleaning service for the bank

v. **Procurement management**:- offices which carry our procurement process for the bank

vi. **Human resource**:- carried out managing the human resource of the bank

vii. **Information system department** :- controls the overall information technology works in the bank

viii. **Internal audit**: - a department which is in charge of controlling the financial operation and analysis.

ix. **Legal service**:- perform legal issues in the bank

x. **Guests:** - a person or an organization whom invited by the bank for business sake.

5.3.1.2.2 Stakeholders Business Correlation with Risk Management Process

- IBR01:- is a Business Relationship between Bank's top level management to Risk management process
- IBR02:- is a Business Relationship between Bank's branch offices to Risk management process
- IBR01:- is a Business Relationship between Bank's other departments to Risk management process
- IBR01:- is a Business Relationship between Bank's security services to Risk management process
- IBR01:- is a Business Relationship between procurement management to Risk management process
- IBR01:- is a Business Relationship between Bank's human resource to Risk management process
- IBR01:- is a Business Relationship between Bank's information system department to Risk management process
- IBR01:- is a Business Relationship between Bank's internal audit to Risk management process
- IBR01:- is a Business Relationship between Bank's legal service to Risk management process
- IBR01:- is a Business Relationship between Bank's guests to Risk management process

5.3.2 Information Security Asset Identification and Characterization

Asset identification and characterization is the second step in the proposed framework. Asset identification Group the information systems, whether internal or external, into categories and differentiate their processes according to their characteristics such as hardware, software, service or policy and regulations. And identifiable collection of data stored in any manner and recognized as having value for the purpose of enabling an agency to perform its business functions, thereby satisfying a recognized agency requirement.

Information security is associated with identified assets. All activities related to information security – security controls, disaster recovery and business continuity programs, and risk assessments, should revolve around protecting the confidentiality, integrity, and availability of the assets of the organization. Unsatisfactory asset identification can leave valuable assets unprotected while the organization spends time on protecting low value resources. Identifying and classifying assets is therefore the foundation of an information security program [14].

Asset characterization is divided in to four major parts as:

- **Information Assets**

Every piece of information about the organization falls in this category. This information has been collected, classified, organized and stored in various forms.

- Databases: Information about customers, personnel, production, sales, marketing, finances. This information is critical for business operation. It's confidentiality, integrity and availability is of utmost importance.
- Data files: Transactional data giving up to date information about each event.
- Operational and support procedures: These have been developed and provide detailed instructions on how to perform various activities.
- Archived information: Old information that may be required to be maintained by law.
- Continuity plans, fallback arrangements: These would be developed to overcome any disaster and maintain the continuity of business. Absence of these will lead to ad-hoc decisions in a crisis.

- **Software Assets**

These can be divided into two categories:

- Application software: Application software implements business rules of the organization. Creation of application software is a time consuming task. Integrity of application software is very important. Any fault in the application software could impact the business adversely.
- System software: banks would invest in various packaged software programs like operating systems, DBMS, development tools and utilities, software packages, office productivity suites etc.

Most of the software under this category would be available off the shelf, unless the software is obsolete or non-standard.

- **Physical Assets**

These are the visible and tangible equipment and could comprise of:

- Computer equipment: Mainframe computers, servers, desktops and notebook computers.
- Communication equipment: Modems, routers, and fax machines.
- Storage media: disks, CDs and DATs.
- Technical equipment: Power supplies, air conditioners.

- **Services**

- Computing services that the organization has outsourced.
- Communication services like voice communication, data communication, value added services, wide area network etc.
- Environmental conditioning services like heating, lighting, air conditioning and power.

5.3.3 Parameter Identification

The parameter we choose is considered as a tool to measure the asset which angle is referred to measure. The researchers' spotlight is these four major constraints:-

- **Confidentiality**

Confidentiality of information is all about protecting the information from disclosure to unauthorized parties.

Information has value, especially in today's world, Bank account statements, personal information, credit card numbers, trade secrets, government documents. Everyone has information one wish to keep a secret. Protecting such information is a very major part of information security.

- **Integrity**

Integrity of information refers to protecting information from being modified by unauthorized parties. Information only has value if it is correct

- **Availability**

Availability of information refers to ensuring that authorized parties are able to access the information when needed. For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

- **Authentication**

It is the authentication of users and administrators in the system.

5.3.4 Threat Identification

The threat identification process would pass through the following process:

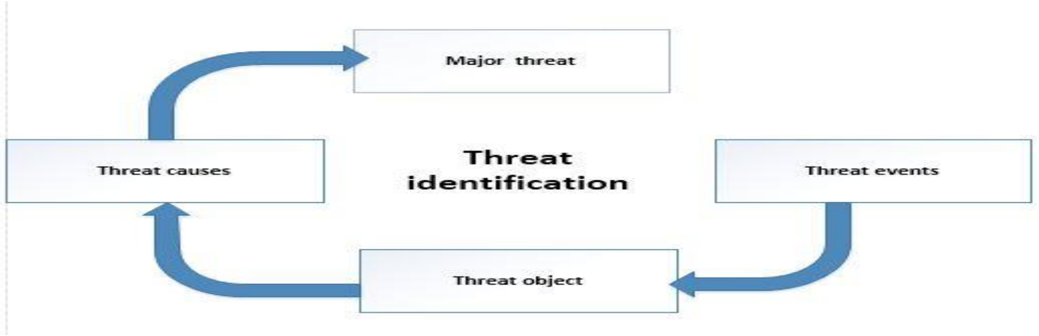


Figure 5.4: Threat Identification Process

- Collecting information: - collecting data regarding identified assets is the first step to threat identification.
- Identifying threats: - is a process of identifying threats from the collected data set.
- Threat events:-are the situations which the threat is possibly occurred
- Threat objects: - the possessions where threats would influence

- Threat cause:-the reason that threat is probably could happen
- Major threat: - the main threat which is identified

5.3.5 Relating Threats with Assets

After identifying existed threats which might make disaster to the system banks should relate those threats with identified assets because asset threat relationship is a major task in risk assessment or risk management process.

5.3.6 Vulnerability Analysis

Vulnerability analysis is to increase awareness and knowledge for decision makers, as well as creating a basis for their own planning. The basis, moreover, constitutes an important source of information for employees. Vulnerability analyses also contribute to providing a picture of the risks and vulnerabilities that exist in the bank in general.

Activities undertaken in vulnerability analysis:

- Identify the Applications and Data that Underline Business Processes

Identify the applications and data on which those mission-critical processes depend. Again, this can be accomplished only through collaboration between IT and other departments in the bank.

- Find Hidden Data Sources**.**

Work with the business units to understand who is using mobile devices for accessing and sharing corporate applications and data. Understand the data flows between these devices and data center applications and storage. Find out if banking users are sending business emails over public email services such as Gmail or Yahoo mail. Another often hidden category to investigate is internal software development environment, as they are inherently less secure than production environments. Software developers and testers often use current, sometimes mission-critical data to test new and upgraded applications.

- Identify which Security Controls are Already in Use

Consider the security and business continuity measures which are already put in place including policies, firewalls, application firewalls, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), data loss prevention and encryption to protect each set of servers and storage devices hosting mission-critical applications and data. Understand the key capabilities of these protections, and which vulnerabilities they address most effectively. This may require some fairly extensive research, including scanning websites and reviews, and speaking with security company representatives.

- Referring Previous Risk Assessment Results

Referring previously developed risk assessment results to make vulnerability analysis.

5.3.7 Impact Study

Impact analysis is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency and so on. Impact is also the degree to which the mission of the bank is damaged by a successful attack from the identified threat.

Impact study also predicts the consequences of disruption of information process by gathering information needed to develop recovery strategies in risk assessment.

The following information is required before conducting an impact analysis.

- System mission e.g. the process performed by IT system.
- System and data criticality e.g. the system's value or importance to an organization System and data sensitivity

Table 5.3: Impact Category

Impact Category	**Definition**
Loss of Revenue	Loss of income received from selling goods or services
Additional Expenses	Temporary staffing, overtime, equipment, services
Regulatory and Legal	Fines, penalties, compliance issues, contractual obligations, financial liabilities
Customer Service	Termination or reduction of service level (internal of external), live operators vs. automated response
Goodwill /Reputation	Public image, shareholder relations, market share

Table 5.3: Impact Ratings

Rating	Impact rate	Description
1	Low	The consequences of loss is low and it could be treated in a short time
2	Medium	The consequences of danger might occur a loss of additional expenses
3	High	The impact is high and might result a high monetary or reputational e.t.c loss
4	Very-high	The impact is very critical and the loss would make the business fail or bankrupt.

5.3.8 Possibility (Probability) Study

This is the process of determining the probability of occurrence of identified threats for the specified assets; it should be done by rating all possible threats.

Table 5.3: Probability Ranking

Rating	Probability of Occurrence	Description
1	Low	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	Medium	Not expected, but there's a slight possibility it may occur at some time.
3	High	The event might occur at some time as there is a history of casual occurrence.
4	Very high	There is a strong possibility the event will occur as there is a history of frequent occurrence.

5.3.9 Risk Prioritization

Risk impact assessment is the process of assessing the probabilities and consequences of risk events if they are realized. The results of this assessment are then used to prioritize risks to establish a most to least critical importance ranking. Ranking risks in terms of their criticality or importance provides insights to the project's management on where resources may be needed to manage or mitigate the realization of high probability/high consequence risk events.

Table 5.3 : Risk Prioritization

	Low impact=1	Medium impact=2	High Impact=3	Very High Impact=4
Low probability of occurrence=1	🟩 **1**	🟩 **2**	🟩 **3**	🟨 **4**
Medium probability occurrence =2	🟩 **2**	🟨 **4**	🟨 **6**	🟨 **8**
High probability occurrence =3	🟩 **3**	🟨 **6**	🟥 **9**	🟥 **12**
Very high probability occurrence =4	🟨 **4**	🟨 **8**	🟥 **12**	🟥 **16**

Note: Red labeled is a high risk zone, Yellow labeled are a medium risk zones and Green labeled are a low risk zones.

5.3.10 Evaluation

After prioritizing risks (assessment) evaluating the process should come at the front. Risk assessment evaluation is a managerial responsibility because once the assessment has done banking top level managers should evaluate the results to make decisions.

It could be done by comparing the estimated result with the final assessment results.

External components: are components of the projected framework which are merely scoped outside the risk assessment team responsibility.

5.3.11 Risk Communication

Risk communication is exchange of information advice and opinions between experts, officials and departments who face a threat to their security. It helps to enable informed decision-making and adopt a defensive mechanism.

5.3.12 Documentation

Following all these process documentation should include objectives, information sources, assumptions, and decisions. Mitigation methodologies should be pointed out for future works.

After communicating and documenting the risk assessment results risk management process need to be continued and it should be an input for the banks future strategies regarding information security.

Generally, Unlike other frameworks such as NIST, ISO, COBIT and OCTAVE the proposed framework is more easy to understand for all employees weather they are professionals or not.

The metric that has been concluded from the result is:-

Asset =should be identified by the employee (Risk assessment team)

Parameters =could be identified by employees (authentication, availability, confidentiality and so on)

Threats= threat event*threat cause*threat object

Impact= degree of loss of the threat (reputational, financial and human)

If impact= very high and probability =very high then prioritize the risk

Risk = impact of the threat * probability of the threat * vulnerability of the asset

5.4 Framework application

Private and public banks in Ethiopia can use the proposed framework by implementing the components procedurally. Risk assessment registry (Appendix D) has been developed. The risk assessment team can fill the registry form to get a result which could finally be an input for risk management process.

CHAPTER SIX

EVALUATION OF THE PROPOSED ICSRA FRAMEWORK

6.1 Introduction

This chapter illustrates the implementation and evaluation process undertaken in the sampled banks. It is tried to demonstrate the proposed framework for those sampled banks in order to improve the validity of the system using the following usage scenario. The developed framework has been demonstrated in three sampled banks.

6.2 Evaluation Feedbacks Obtained

As Banks implemented and remarked on the proposed framework comments and suggestions have been raised in different contents of the framework.

Figure 6.1 presents the adopted framework for bank experts so it is simpler to use or apply in their context. It clearly shows the inputs, process and outputs for each stage as they progress in evaluating their bank's information and cyber risks.

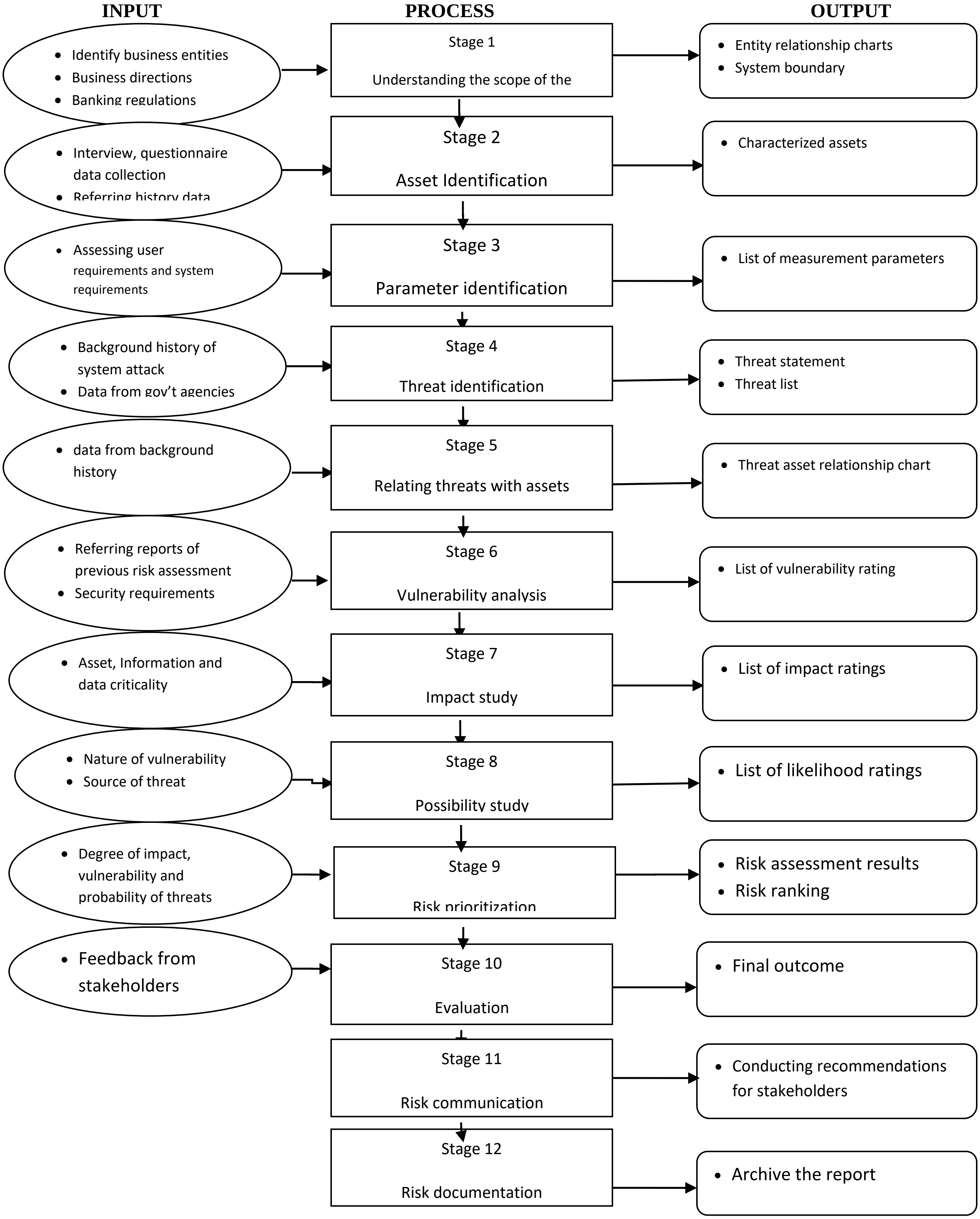

INPUT
PROCESS
OUTPUT
Identify business entities
Business directions
Banking regulations
Stage 1
Understanding the scope of the
Entity relationship charts
System boundary
Interview, questionnaire data collection
Referring history data
Stage 2
Asset Identification
Characterized assets
Assessing user requirements and system requirements
Stage 3
Parameter identification
List of measurement parameters
Background history of system attack
Data from gov't agencies
Stage 4
Threat identification
Threat statement
Threat list
data from background history
Stage 5
Relating threats with assets
Threat asset relationship chart
Referring reports of previous risk assessment
Security requirements
Stage 6
Vulnerability analysis
List of vulnerability rating
Asset, Information and data criticality
Stage 7
Impact study
List of impact ratings
Nature of vulnerability
Source of threat
Stage 8
Possibility study
List of likelihood ratings
Degree of impact, vulnerability and probability of threats
Stage 9
Risk prioritization
Risk assessment results
Risk ranking
Feedback from stakeholders
Stage 10
Evaluation
Final outcome
Stage 11
Risk communication
Conducting recommendations for stakeholders
Stage 12
Risk documentation
Archive the report

Figure 6.1: Framework Input, Process and Output Flow Chart

6.2.1 ICSRA Evaluation by Bank 1

Following the demonstration given about how the framework can be used in Bank 1, domain experts from concerned departments has been participated to put into practice the developed framework. By means of introducing the system to the existing environment to assess information and cyber security risks.

The team followed the whole stages which are projected in the framework to put into operation. Primarily, the team has identified the scope which is already developed by the researcher previously during data collection plus the parameters they used were Integration, confidentiality and availability. The assessment team has used a risk assessment registry Appendix D which is developed by the researcher.

In Bank 1 the assessment team has identified assets such as Data base server, Communication devices and end user (desktop) computers. All identified threats have been registered in the registry form and corresponding threats of each asset have been listed out. The team has encompassed vulnerability, impact and likelihood studies in two weeks in a row.

Eventually, the team prioritized risks which have very high impact, vulnerability and likelihood. As well. Communication and documentation process have been done accordingly. During assessment the tram has also identified observable limitations such as:

- On the second component of the framework “Parameter Identification” the term should be clear and understandable.
- The framework should be stated in a way that all professionals or non professionals to understand each procedures.

6.2.2 ICSRA Evaluation by Bank 2

In Bank 2, even though there is no a risk assessment expert’s, officers from Information Security department has participated to implement and evaluate the framework regarding the general components and what it should be like as well as how the components are organized to make the result reliable and consistent.

Bank 2 has organized a risk assessment team from three departments like Information Security, Network Administrators and System Administrators. The team has five members; three from information security department and one from network the other one from system administrators department.

In the first day, the team has had a meeting to discuss about how to initiate and how to go on the risk assessment process. And the researcher gave a short description on how to exercise the framework as it has proposed.

Afterward, the team recognizes the researchers developed scope. Database server and Networking devices are selected as an asset. Parameters chosen to be evaluated are Availability; Confidentiality and Integrity. Subsequently, threats are listed by collecting data from background history of documented files and interviewing related domain experts. Then linking those threats with their corresponding assets have been done.

Following relating assets with their corresponding threats, vulnerability analysis was followed. Impact and possibility (likelihood) analysis have been done together with determining risk score to help prioritize risks which are very high impact and very high likelihood.

Ultimately the risk assessment team reported all results to Information security department. While doing assessment the team has commented the researcher to make:

- Components short and precise

6.2.3 ICSRA Evaluation by Bank 3

Even though, Bank 3 has Risk management division, it uses government agencies recommendations as well informal methods to assess its risk. In risk management division there is a risk assessment team which does risk assessment.

Bank 3 has scheduled risk assessment team to work with the researchers proposed framework. The team inquired information about how to do the assessment process and what are the inputs for all components and what is the expected output from each process.

The researcher provided all necessary information like input, process and output chart for the team and the team began its assessment process. The initial step was scope identification; it was already done by the researcher back in framework development time. Assets were identified by referring documented files those are: Database Servers, End Users, Networking devices, Data centers and monetary information. Availability, Integrity, Authentication and Confidentiality are identified parameters to be evaluated.

Identifying threats and relating those threats with the corresponding asset was the next task. After relating all identified threats with their related asset; the successive activity was vulnerability analysis it was done using these techniques;

- Finding hidden data sources
- Identifying the applications and data that underline business processes
- Identifying which security controls are already in use
- Referring previous risk assessment results

Subsequently, possibility and impact analysis was done to determine the likelihood and consequences of the risk. And then finally risk score has been completed using risk score table which the researcher provided in advance.

Finally, risk prioritization has been made referring risk score results. Evaluation was done by the assessment team by comparing with previously assessment results also the team sent the results and outcomes to the risk management division.

6.3 Discussion

To achieve the preliminary objective of this research the researcher has directly involved collecting data from the stakeholders of different areas of the banking sector.

The framework process could be achieved by filling the risk assessment framework registry (APPENDIX D). The risk assessment team shall follow the registry format to easily accomplish the risk assessment.

Thus the data collected from the experiment group has been used as an input to develop the framework and to make it for banks in Ethiopia.

The researcher has achieved the goals by implementing and testing the proposed framework in the sampled banks. The results incurred during implementation of the framework were fruitful as compared with other currently applicable (which are informally suggested from INSA).

As observed from banks after implementation and validation of the framework, suggestions and feedbacks are collected.

The evaluation process was detained in 3 sampled banks which are previously sampled to assemble data during data collection process. Domain experts, risk management team and Information Security officers have been participated to implement and evaluate the framework. All necessary procedures have been done using risk registry form Appendix D.

Subsequent to, accumulating all results and outcomes observed form these 3 sampled banks it could be easy to conclude the projected framework was successfully developed since the demonstration process was effectively completed. Additionally sampled banks suggested the researcher to convey this framework in all currently operational banks in Ethiopia.

CHAPTER SEVEN

CONCLUSIONS AND RECOMMENDATIONS

7.1 Conclusions

In this study it is developed a new framework for information and cyber security risk assessment of a banking system in Ethiopia.

The conceptual framework comprised of ten components. Unlike, other frameworks, it considers Ethiopian external entities interacted with both private and public banks.

RM studio was used to assess the surveyed banks which use four major processes to develop the ICSRA framework different researchers followed different techniques and procedures. Some researcher's done by précising the process by combining practices. This research has been made considering the possible stakeholders to the banks and internal relationship with departments in the banks. ISO, NIST, OCTAVE and other methodologies were consulted which are developed for considering European and American financial and government policy.

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

The components which are included in the projected framework are presented as:-understanding of the system, parameter identification, and asset identification, threat identification, relating threats with assets, vulnerability analysis, impact study, risk prioritization, evaluation, risk communication and documentation.

To conclude, the developed risk assessment framework helped banks in Ethiopia to assess information and cyber security risk which could harm the banks information security environment.

7.2 Recommendations

The developed conceptual framework could be a preliminary input to the banks to assess their risk and prioritize the risks to develop countermeasure policies. And, for researchers it could be a reference to develop a mitigation policy.

This study covered one of the most critical areas in the risk management process. So, researchers and banks can use it as:-

- Development instrument to devise risk treatment strategy
- A prior input for researchers to develop risk mitigation policy
- Banks can easily use it to develop risk portfolios assessment by their officers without consulting external entities.
- A tool for the banks to review their information security assets, resources and policies.

References

[1] T. juan, ""RiskAssessment of Computer Network Security in Banks"," pp. 5-11, 2016.

[2] A. Weretaw, ""Information security culture in the banking sector in Ethiopia"," in *Information Network Security Agency*, Addis Ababa, 2012.

[3] “. a. I. S. i. t. F. Sector, "enisa," ENISA, (2014. [Online]. Available: www.enisa.europa.eu.. [Accessed 9 7 20017].

[4] D. S. A. M. P. Abdella Kossa, "Risk Assessment and Handling in Ethiopian Commercial Banks: A Comparative Study of Public and Private Sectors", Addis Ababa, 2016.

[5] K. tebikew, ""Information Security Management Framework for Banking Industry in Ethiopia"," 1 7 2013. [Online]. Available: www.aau.edu.et. [Accessed 30 7 2017].

[6] I. M. Usman Munir, "Information Security RIsk Assessment for the Banking Sector- Acase study of Pakistani Banks", Islamabad, 2010.

[7] Stavroula, "Risk management in banking; the case of Greek banking industry", Department of Balkan, Slavic and Oriental studies, University of Macedonia, 2009.

[8] Wie, ""Analysis of Computer Network Security"," *Guangxi Journal of Light Industry,* 2007.

[9] L.Bingqi, ""The Factors Influencing the Computer Network Security and Countermeasures"," in *Computer Engineering & Software*, 2009.

[10] P. r. m. Association, ""Enterprise Risk Management (ERM) and the requirements of ISO 31000”AIRMIC, Alarm, and IRM"," Public Risk Management Association, 2010.

[11] Lee, ""Risk Management Metrics and Risk Assessments"," *Enterprise Risk Management,* vol. 200, p. 40, 2008.

[12] T. Stephanou, "Assessing and Exploiting the Internal Security of an Organization", The SANS Institute, 2001.

[13] I. M. Usman Munir, Information Security Risk Assessment for Banking Sector-A Case study of Pakistani Banks, 2010.

[14] CANSO, ""Cyber Security and Risk Assessment Guide"," 2014.

[15] NIST, "Risk Management Guide for Information Technology Systems," 2002.

[16] Bitsightech, "BItsightech," 2017. [Online]. Available: https://www.bitsighttech.com . [Accessed 9 7 2017].

[17] N. ITS, ""Information Security Risk Management"," 2015.

[18] F. f. i. examination, ""Information Security"," Federal financial institutions examination, 2006.

[19] S. Zhang, A model for evaluating computer network security systems with 2 tuple linguistic information, 2011, pp. 62-71.

[20] T. V. Estévez Tapiador, "A computer system descrptionframework and its application to network security", 2003.

[21] D. lonita, "Current Established Risk Assessment Methodologies and Tools," in *Current Established Risk Assessment Methodologies and Tools*, July 2013, pp. 46-68.

[22] SANS, "Security spending and preparedness in financial secto," SANS, 2015.

[23] IBM, ""Security over view Cloud Computing"," 2009.

[24] H. Takabi, ""Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments"," in *IEEE 34th Annual Conference on Computer Software and Application*, July 2010.

[25] I. 2001-2, "www.ISO.org," 2005/2013. [Online]. Available: https://www.iso.org/standard/42103.html.

[26] L. N. &. A. L. S. Anene, "An Architectural and Process Model Approach to Information Security Management", Lawrence Technological University, 2007.

[27] Y. T. Damenu, cyber security risk assessment framwerok for banking sector of ethiopia, Addis Ababa: HiLCoE, 2017.

APPENDIX A: Questionnaire

Respondent's background information:-

1) Gender: male ( ) female ( )

2) Age group

18-24 ( ) 25-30 ( ) 31-35 ( ) 36-40 ( ) 41-45 ( ) above 45 ( )

3) Qualification

10+2 ( ) 12+2 ( ) BSc/BA ( ) MSc/MA ( ) PhD ( )

4) Job title____

5) Year of service in the banking industry

0-1 year ( ) 1-2 years ( ) 2-5 years ( ) 5-10 years ( ) >10years ( )

6) Year of service in your current position

0-1 year ( ) 1-2 years ( ) 2-5 years ( ) 5-10 years ( ) >10years ( )

Section I:-General questions regarding your business resource.			
Questions	***Yes***	***No***	***I don't know***
1. Is your web application resource hosted by a third party?	**Yes ( )**	**No ( )**	**N/A( )**
2. Did you do Resource Inventory for any system that is storing, processing, or transmitting financial (monetary) information? If yes when and how often did you do?	**Yes ( )**	**No( )**	**N/A( )**
Section II:-This category includes questions regarding any network infrastructure (routers, firewalls, switches) supporting the servers (OPERATION).			
3. For servers not hosted in ______Bank data centers, are any servers under your control storing sensitive information such as financial information and financial transactions?	**Yes ( )**	**No( )**	**N/A( )**

4. Is an ISO approved patching application used and configured to run on all servers?	**Yes ( )**	**No( )**	**N/A( )**
5. Do server administrators install software downloaded from the Internet?	**Yes( )**	**No ( )**	**N/A( )**
6. Is an antivirus program running on all servers?	**Yes ( )**	**No( )**	**N/A( )**
7. Is port access allowed to servers from other Bank networks?	**Yes ( )**	**No( )**	**N/A( )**
8. Is port access allowed to servers from public Internet?	**Yes ( )**	**No( )**	**N/A( )**
9. Are administrative privileges for networked devices controlled?	**Yes ( )**	**No( )**	**N/A( )**
10. Have the systems been reviewed to be following the Event Monitoring Security standard? If yes, please list date verified	**Yes ( )**	**No( )**	**N/A( )**
11. Does the implemented security event logging solution detect and alert on security events? If yes in how many hours or minutes?	**Yes ( )**	**No ( )**	**N/A( )**
12. Is event monitoring enabled for security relevant events?	**Yes ( )**	**No( )**	**N/A( )**
13. Are security events monitored and analyzed on a daily basis? If no How often?________________________	**Yes ( )**	**No( )**	**N/A( )**

14. Are security events retained for the required maintenance period, by mirroring to a separate logging server?	**Yes ( )**	**No ( )**	**N/A( )**
15. Is a device tracking inventory control system in place to track all hardware on the network so that only authorized devices are given access, and unmanaged devices are found and prevented from gaining access?	**Yes ( )**	**No ( )**	**N/A( )**
16. Is a change control system in place for tracking and managing any changes to routers, firewalls, and switches?	**Yes ( )**	**No( )**	**N/A( )**
17. Are ACLs enforced on the servers to prevent unauthorized copying or writing of sensitive information?	**Yes ( )**	**No ( )**	**N/A( )**
18. Can the servers detect all attempts to access files on local systems or network file shares with the appropriate privilege?	**Yes ( )**	**No ( )**	**N/A( )**
19. Have you completed the Resource Inventory for any web application storing, processing, or transmitting financial (monetary) information?	**Yes ( )**	**No ( )**	**N/A( )**
20. Has the web application undergone a web application security assessment? If yes, how often do you do?	**Yes ( )**	**No ( )**	**N/A( )**
21. Does the web application require forms for authentication of user credentials with different authorization levels?	**Yes ( )**	**No ( )**	**N/A( )**
22. Does the web application server dynamic	**Yes ( )**	**No ( )**	**N/A( )**

content using a backend database connection?			
23. Is the web application protected with a firewall and located behind a DMZ?	**Yes ( )**	**No ( )**	**N/A( )**
24. Has a web application firewall been installed and properly tuned, to help provide threat mitigation against attacks against the web applications?	**Yes ( )**	**No ( )**	**N/A( )**
Section III:-This section includes questions regarding all endpoints and users. Endpoints include workstations, laptops, and mobile computing machines. The users include both regular users and Administrators that have access to sensitive information.(infrastructure and users)			
25. Does the information owner or delegate assign and review permissions for user application access to financial (monetary) information on a periodic basis?	**Yes ( )**	**No ( )**	**N/A( )**
26. Is the principle of least privilege used when assigning permissions to users for business applications that need access to financial (monetary) information?	**Yes ( )**	**No ( )**	**N/A( )**
27. Does your users' access highly sensitive information? If yes, what applications or client applications are used?	**Yes ( )**	**No ( )**	**N/A( )**
27.1 For question no.27 (For any of these applications): do they currently store, process, or transmit any sensitive information unencrypted?	**Yes ( )**	**No ( )**	**N/A( )**
28. Is financial and monetary information stored on workstation (including laptops	**Yes ( )**	**No ( )**	**N/A( )**

and mobile computing devices) hard drives encrypted?			
29. Is financial (monetary) information stored on exchangeable media (USB, CD/DVD) encrypted?	**Yes ( )**	**No ( )**	**N/A( )**
30. For any machines decrypting Financial (monetary) information: Are these machines running an ISO approved antivirus application?	**Yes ( )**	**No ( )**	**N/A( )**
31. Is storage of any Financial (monetary) information taking place on any cloud based storage systems such as Google drive or drop box?	**Yes ( )**	**No ( )**	**N/A( )**
32. Is personal email used to transmit financial (monetary) information?	**Yes ( )**	**No ( )**	**N/A( )**
33. From the Internet, are any inbound connections allowed directly through the firewall into any workstation, laptop, or mobile computing machines under your control? If yes, please list exceptions	**Yes ( )**	**No ( )**	**N/A( )**
34. From other Bank networks, are any other networks allowed through firewall to access services on your machines?	**Yes ( )**	**No ( )**	**N/A( )**
35. Do any users run patching applications other than ISO approved?	**Yes ( )**	**No ( )**	**N/A( )**
36. Do any users run Antivirus applications	**Yes ( )**	**No ( )**	**N/A( )**

other than ISO approved?			
37. Are any endpoints running an Operating System that is not supported by the vendor, such as Windows XP? If yes, please list exceptions	**Yes ( )**	**No ( )**	**N/A( )**
38. Has a random sampling of the laptops or workstations been screened for the existence of stored sensitive data that is unencrypted?	**Yes ( )**	**No ( )**	**N/A( )**
39. Do users log in with administrative credentials on workstations or laptops? If yes please list exception reasons:	**Yes ( )**	**No ( )**	**N/A( )**
40. Is Administrative privilege granted by business owners with the principle of least privilege?	**Yes ( )**	**No ( )**	**N/A( )**
41. Do users install software downloaded from the Internet? If yes, please list exception reason:	**Yes ( )**	**No ( )**	**N/A( )**

42. The initial distribution of passwords, password lockout and password reset follows the ISO password standard?	**Yes ( )**	**No ( )**	**N/A( )**
43. For endpoints: Is a device tracking inventory control system in place to track all hardware on the network so that only authorized devices are given access, and unmanaged devices are found and prevented from gaining access?	**Yes ( )**	**No ( )**	**N/A( )**
44. Is a Data Loss Prevention solution in place to prevent data ex filtration of sensitive financial (monetary) information?	**Yes ( )**	**No ( )**	**N/A( )**
45. Has an incident response infrastructure, program, or process been developed so that information owners and administrators can respond to security incidents with the help of ISO?	**Yes ( )**	**No ( )**	**N/A( )**
Section IV: - This section includes questions related to integrity, authorization and availability of information resources; should be rated as low, high, or very high.			
Low:-Resulting in minimal monetary, productivity, or reputational losses **High: -**Resulting in certain monetary, productivity, or reputational losses. **Very high: -**Resulting in significant monetary, productivity, or reputational lose			
	Low	**High**	**Very high**
1. Please rate the overall confidentiality needs (the consequences of unauthorized disclosure or compromise of data stored, processed, or transmitted by the resource) of the information resource.			
2. Please rate the overall integrity needs (basically the consequences of corruption or unauthorized modification/destruction			

of data stored, processed, or transmitted by the resource) of the information resource.			
3. Please rate the overall availability needs (basically the consequences of loss or disruption of access to data the resource stores, processes or transmits) of the information resource to ***non-Bank users.***			
4. Please rate the overall availability needs (basically the consequences of loss or disruption of access to data the resource stores, processes or transmits) of the information resource to ***Bank users.***			

APPENDIX B: Interview Questions

1. What kind of IT risk management methodology or standard you have used if not does you bank developed any RA/RM framework?

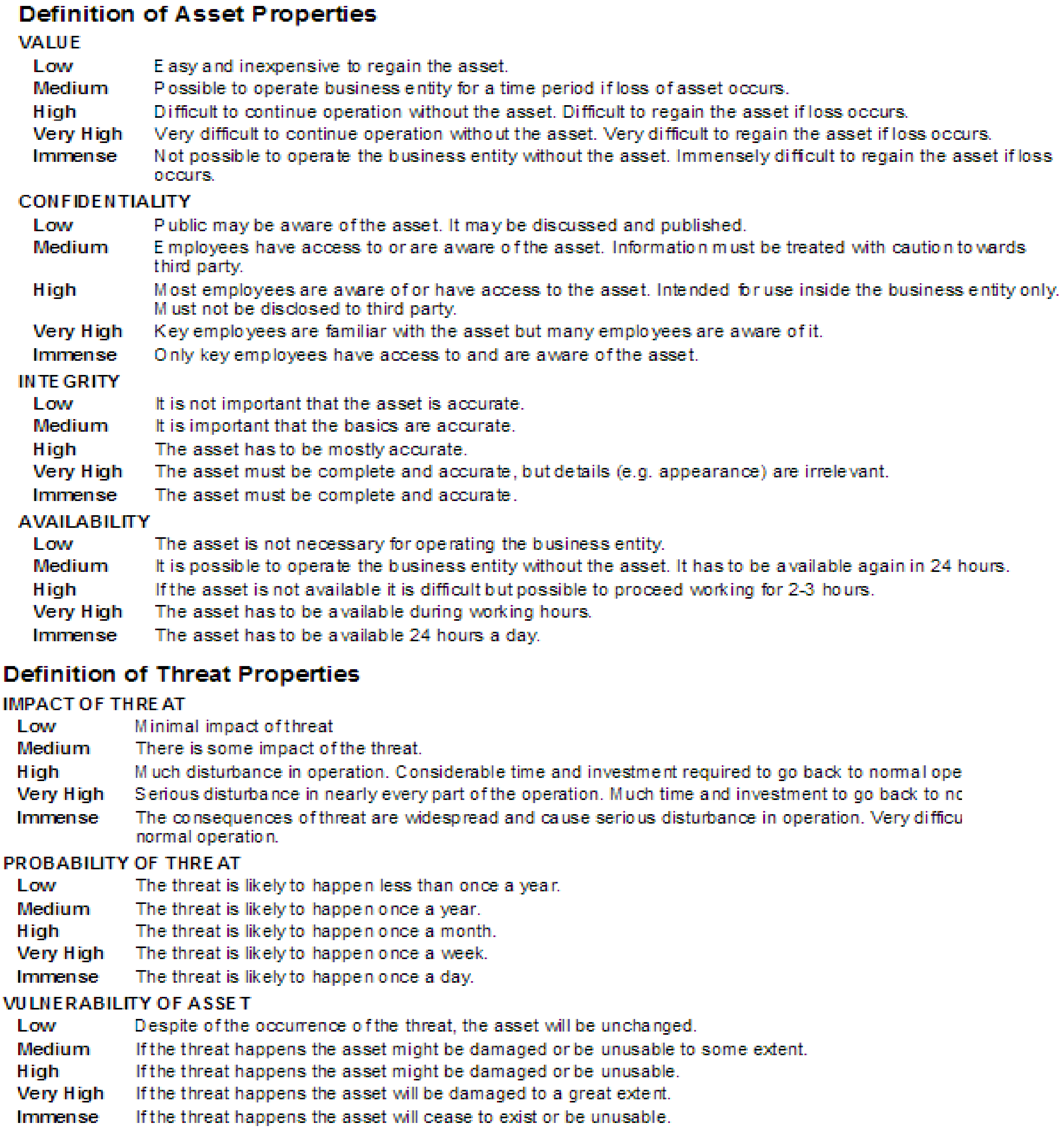
2. Does your organization implement a risk assessment?

3. Does your organization ever faced with any kind of external or internal attack?

4. What do you suggest for banks to deploy a risk management process?

5. What are the disadvantages and strengths of the model that you have employed for?

APPENDIX C: Definition of Asset and Threat Definition



Definition of Asset Properties

VALUE

Low	Easy and inexpensive to regain the asset.
Medium	Possible to operate business entity for a time period if loss of asset occurs.
High	Difficult to continue operation without the asset. Difficult to regain the asset if loss occurs.
Very High	Very difficult to continue operation without the asset. Very difficult to regain the asset if loss occurs.
Immense	Not possible to operate the business entity without the asset. Immensely difficult to regain the asset if loss occurs.

CONFIDENTIALITY

Low	Public may be aware of the asset. It may be discussed and published.
Medium	Employees have access to or are aware of the asset. Information must be treated with caution towards third party.
High	Most employees are aware of or have access to the asset. Intended for use inside the business entity only. Must not be disclosed to third party.
Very High	Key employees are familiar with the asset but many employees are aware of it.
Immense	Only key employees have access to and are aware of the asset.

INTEGRITY

Low	It is not important that the asset is accurate.
Medium	It is important that the basics are accurate.
High	The asset has to be mostly accurate.
Very High	The asset must be complete and accurate, but details (e.g. appearance) are irrelevant.
Immense	The asset must be complete and accurate.

AVAILABILITY

Low	The asset is not necessary for operating the business entity.
Medium	It is possible to operate the business entity without the asset. It has to be available again in 24 hours.
High	If the asset is not available it is difficult but possible to proceed working for 2-3 hours.
Very High	The asset has to be available during working hours.
Immense	The asset has to be available 24 hours a day.

Definition of Threat Properties

IMPACT OF THREAT

Low	Minimal impact of threat
Medium	There is some impact of the threat.
High	Much disturbance in operation. Considerable time and investment required to go back to normal ope
Very High	Serious disturbance in nearly every part of the operation. Much time and investment to go back to nc
Immense	The consequences of threat are widespread and cause serious disturbance in operation. Very difficu normal operation.

PROBABILITY OF THREAT

Low	The threat is likely to happen less than once a year.
Medium	The threat is likely to happen once a year.
High	The threat is likely to happen once a month.
Very High	The threat is likely to happen once a week.
Immense	The threat is likely to happen once a day.

VULNERABILITY OF ASSET

Low	Despite of the occurrence of the threat, the asset will be unchanged.
Medium	If the threat happens the asset might be damaged or be unusable to some extent.
High	If the threat happens the asset might be damaged or be unusable.
Very High	If the threat happens the asset will be damaged to a great extent.
Immense	If the threat happens the asset will cease to exist or be unusable.

APPENDIX D : Risk Assessment Registry for Private and Public Banks

ICS Risk Assessment Registry:

Date: _____/______/_____ Reference Num:-

Work sheet No.		Assessment time:				Assessed by:
Parameter values						
S/N	Asset Name	Availability	Integrity	Confidentiality	Authentication	Remarks
1						
2						
3						
4		.				
5						
6						

ICS RISK ASSESSMENT REGISTRY

Threat list

S/N	Threats	Remarks
1		
2		

Threat Asset Relationship

S/N	Asset	Related Threat
1		

ICS RISK ASSESSMENT REGISTRY

Vulnerability Analysis

S/N	Asset	Related Threat	Vulnerability Analysis
1			

Possibility and Impact Analysis

S/N	Asset	Related Threat	Probability ranking	Impact result
1				

ICS RISK ASSESSMENT REGISTRY

Risk Score

	Low impact=1	Medium impact=2	High Impact=3	Very High Impact=4
Low probability of occurrence=1	**1**	**2**	**3**	**4**
Medium probability occurrence =2	**2**	**4**	**6**	**8**
High probability occurrence =3	**3**	**6**	**9**	**12**
Very high probability occurrence =4	**4**	**8**	**12**	**16**

Risk Prioritization

S/N	Asset	Related Threat	Ranking	Remarks
1				

ICS RISK ASSESSMENT REGISTRY

Note: Instruction of Filling

1. Parameter values are “LOW”, “MEDIUM”, “HIGH” and “VERY HIGH”.
2. Risk prioritization is done by numbering such like (1, 2, 3, 4….).
3. Probability analysis and impact analysis values are “LOW”, “MEDIUM”, “HIGH” and “VERY HIGH”.

Standard History Tracking			
SN	Standard name	Prepared by	Date:
1	Information and Cyber Security Risk Assessment for the Banking sector in Ethiopia	Biniyam Wedelu	December /2017