Seek Wisdom, Elevate your Intellect and Serve Humanity

Addis Ababa University
አዲስ አበባ ዩኒቨርሲቲ

ADDIS ABABA UNIVERSITY SCHOOL OF COMMERCE

MA Program in Project Management

Assessment of Cyber Security Risk Management Practices: Human factors, and implementation Challenges: In Case of Commercial Bank of Ethiopia (CBE)

By; -FekaduEndrias

Advisor: Teklegiogis Assefa(PHD)

June, 2024

Assessment of Cyber Security Risk Management Practices: Human factors, and implementation Challenges: In Case of Commercial Bank of Ethiopia (CBE)

By

Fekadu Endrias

A Project Research Work in Partial Fulfillment of the Requirements for the Award of Master of Arts Degree in Project Management

Advisor

Teklegiorgis Assefa (PHD)

June, 2024

Addis Ababa, Ethiopia

LETTER OF CERTIFICATION

In partial fulfillment of the requirements for the Masters of Arts in Project Management degree entitled Assessment of Cyber Security Risk Management Practices: Human factors, and implementation Challenges: In Case of Commercial Bank of Ethiopia (CBE), I hereby certify that Fekadu Endrias completed the work under my supervision. Therefore, I recommend that the student submit the project study work to the department as they have met the requirements.

Name of advisor: _____

Signature: _____

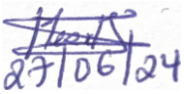
Date: _____

Approval by board of examiners

Project Research Work Title: Assessment of Cyber Security Risk Management Practices:

Human factors, and implementation Challenges: In Case of Commercial Bank of Ethiopia (CBE)

Approved by: Name and signature of members of the Advisor and Examining Board members

Advisor	Signature	Date
Internal Examiner	Signature	Date
Meskerem M (PhD)		
External Examiner	Signature	Date

Declaration

I, Fekadu Endrias, hereby declare that the study I have conducted is entirely my own original work. It has not been submitted to university or other institution for the purpose of earning a degree or for any other reason. I further guarantee that all information sources used in this work have been properly acknowledged.

Name: _____

Signature: _____

Date: _____

Acknowledgment

I sincerely appreciate everyone's assistance and direction in helping me to finish this research work. First and foremost, I want to thank God for giving me the courage, insight, and inspiration to carry out this research.

Additionally, I want to express my gratitude to Teklegiorgis Assefa (PHD), my adviser, for his insightful advice, mentoring, and helpful criticism. His knowledge and experience have been very helpful in forming my research questions, refining my approach, and guaranteeing the validity of my work.

.

My wife in particular deserves special praise for her unwavering support, understanding, and love along this journey on behalf of our family. They have been my constant source of inspiration and drive, sticking by me through good times and bad. Without their support, this research work would not have been possible.

I am also grateful of my friends, coworkers, and research participants who so kindly gave of their time, skills, and knowledge. Their contributions have widened my perspective on the subject and enhanced my research.

Lastly, I would want to thank everyone who has helped me over the years in both my academic and personal development. Your help has greatly influenced who I am now, and I will always be appreciative of your kindness and generosity.

Abbreviations and acronyms

CBE: Commercial bank of Ethiopia

CSRM: Cyber security risk management

SPSS: Statistical Package for Social Sciences

PCI DSS: Payment Card Industry Data Security Standard

GDPR: General Data Protection Regulation

NIST: National Institute of Standards and Technology

Contents

List of Tables

List of Figures

Abstract

This study evaluates the cyber security risk management practices, human factors affecting effectiveness of cyber security risk management and challenges faced by the Commercial Bank of Ethiopia (CBE). Cyber security risk management involves identifying, analyzing, evaluating, and addressing cyber security threats, and it is essential for safeguarding financial assets, preventing fraud, and maintaining trust in the banking system. The research identifies the existing cyber security risk management practices at CBE, the non-technical factors affecting their effectiveness, and the challenges encountered during their implementation.

The study used a quantitative research design to evaluate the issues and present practices through the use of statistical analyses and surveys. The study environment was created by staff members of the Commercial Bank of Ethiopia, and 66 study participants were chosen from the cyber security department using judgmental random sampling SPSS version 26 was used to conduct a quantitative analysis of the data obtained from an open-ended questionnaire, interviews, and a closed-ended questionnaire. Important conclusions show that although CBE has put strong security measures in place, like firewalls and antivirus programs, there are still big gaps in the processes for reporting cyber security issues and communicating with one another. Cyber security practices are not as effective when human variables such as security awareness, training, behavioral issues, and cognitive load are not taken into account. Leadership commitment and organizational security culture are also very important and significantly influence the effectiveness of these practices.

This research provides insights into the cyber security landscape of Ethiopian banks, highlighting areas for improvement and offering recommendations to enhance the overall cyber security posture of CBE. The findings are intended to inform the development and implementation of more robust cyber security frameworks within the Ethiopian banking industry, ensuring compliance with regulatory requirements and fostering trust and resilience in the digital era.

Keywords: Cyber security, risk management, human factors, non-technical factors, organizational culture, leadership.

Chapter One

Introduction

1.1 Background of the Study

Globalization was made possible by the internet, which began as an ARPA Net project in the US Department of Defense and developed into a worldwide network. The global IT infrastructure that powers the internet, a network of networks, is changing the social, political, and economic landscape of the world. According to Desisa and Beshah (2014), individuals have been using the Internet to complete daily tasks more and more since its inception (p.1). Information and communication technology (ICT) networks, devices, and services are becoming more and more essential to daily life, according to the 2017 Global Cyber Security Index (GCI) study (Global Cyber Security Index, 2017, p.1).

Munk (2015) consequently claimed that communications between individuals and groups, as well as all public-private sectors and governmental operations, are all exhibiting a greater reliance on cyberspace (p.7). The worldwide community is embracing ICTs as a critical enabler for social and economic progress, according to the worldwide Cyber Security Index of 2017 study, which supports this further (Global Cyber Security Index, 2017, p.iii). The internet, in particular, has an impact on almost every facet of human existence. According to Munk (2015), every facet of both public and private computing is grounded by the extremely decentralized and more complicated internet (p. 12). The same author went on to say that despite all of its user-friendly appeal and promises, the internet is essentially a "cloud" and "series of tubes" that connects everything from Face book profiles, to bank accounts, to aspects of critical governmental and private infrastructure (p.12). Financial institutions can function at a high degree of efficiency thanks to computer networks. The daily operations of private institutions rely heavily on information technology.

Governments use computer networks and the internet to process, store, and distribute data efficiently. In support of this idea, Bogale (2016) noted that information technology (IT) has become essential to the survival and expansion of businesses in manyorganizations(Bogale,p.25).

The environment of cyber security is defined by an acceleration of digitalization, a rise in cyber threats, and an increasing dependence on digital systems. Numerous threats, such as ransom ware, phishing, malware, and insider assaults, can cause significant financial, operational, and reputational harm to organizations. In order to address these concerns, regulations are changing, yet obstacles like resource shortages and technology complexity persist. Global developments in emerging technologies, such as AI, indicate a variety of threat activity and changing assault strategies. To reduce risks and safeguard sensitive data, businesses must implement strong cyber security measures as they traverse this ever-changing environment. The goal of the bank-specific cyber security environment is to safeguard financial assets, customer data, and vital infrastructure against cyber assaults. Because banks hold valuable information, they are often the target of numerous types of assaults. Breach in the banking industry can have serious repercussions, including money loss, fines, and harm to one's image. Strict guidelines are enforced by regulatory agencies on banks to guarantee the confidentiality and security of client data. In addition, banks deal with issues like outdated systems, intricate networks, limited resources, a lack of skilled workers, and the quick advancement of technology and the need to balance security with convenience for customers. As technology continues to evolve banks, must continuously adapt and strengthen cyber security measure to stay ahead of emerging threats and safeguard the trust of their customers (Siber Risk Sigortası, November 2018)

The safety of financial assets, the privacy of client data, regulatory compliance, reputation preservation, operational resilience, and defense against new threats are just a few of the important reasons why cyber security risk management is important. Overall, the banking industry needs to handle cyber security risks carefully because failing to do so could have negative effects on banks and the larger financial system. (Berger Emanuel Kopp, Lincoln Kaffen, 2019)

Banks employ well-established frameworks, rules, and best practices for cyber security risk management, such as the FFIEC cyber security assessment tools, PCI-DSS, ISO27001, NIST Framework, and PCI-DSS, to overcome and mitigate cyber threats.

The majority of businesses put in place well-established frameworks for cyber security risk management to make sure the most serious threats were dealt with as soon as possible. To analyze the organization's current security posture and security framework, it must, nonetheless, review the current cyber security risk management methods. In today's digital environments, this

evaluation serves as a useful tool for efficiently identifying, reducing, and managing cyber security risks. Organizations must continuously evaluate their cyber security risk management procedures to guarantee their efficacy and resilience as cyber-security threats continue to change and grow more complex.

Cyber security risk management practices include factors like technological infrastructure and investment, regulatory environments, human factors, organizational culture and leadership, external threat landscapes, third-party relationships, incident response and resilience, and data protection and privacy. This variable can group in to five domains on their nature and relevance to cyber security risk management. These are technological infrastructure factors, human factors, regulatory compliance, organizational culture and leadership and incident response and resilience factors.

These five domains also categorized into technical and non-technical variables based on their relevance to technology and their implications for the study context. Technical variables include technological factors, regulatory compliance and incident response and resilience factors the non-technical factors are human factors and organizational culture and leadership (Sekaran and Bougie (2016)).

In summary, this research intends to fill the academic gap by providing a comprehensive assessment of cyber security risk management practices at commercial bank of Ethiopia, focusing on human factors and implementation challenges. By addressing these aspects, the study aims to advance knowledge in cyber security management within the banking sector and contribute practical insights that can benefit both academia and industry stakeholders involved in cyber security governance and operations.

1.2 Background of the organization

The State Bank of Ethiopia was founded in 1942, and that is when the Commercial Bank of Ethiopia (CBE) got its start. In 1963, CBE was formally founded as a share company. CBE and the privately held Addis Ababa Bank amalgamated in 1974. It has continued to have a major impact on the nations development ever since.

CBE was the first in the nation to implement modern banking. Its more than 1280 branches are dispersed around the nation. The top African bank, as of June 30, 2018, with 565.5 billion Birr in assets. It contributes as a catalyst to the nation's economic growth and advancement. The first bank in Ethiopia to offer ATM service to its citizens is CBE.

As of June 30, 2018, CBE had over 18.8 million account holders, and over 1,736,768 people were using its mobile and online banking services. Over 4.4 million ATM cards were in use as of this writing. There were 11,796 POS machines and 1708 ATMs in operation as of June 30, 2018. More than fifty prominent international banks, including Commerz Bank A.G., Royal Bank of Canada, City Bank, and HSBC Bank, have a strong correspondent connection with it.CBE and over 700 other banks worldwide have bilateral SWIFT agreements.

In addition to having a large capital base, CBE employs over 33,000 skilled and dedicated workers. Early in the 1990s, the pioneer in bringing Western Union money transfer services to Ethiopia was also the one collaborating with other twenty money transfer companies, including Money Gram, Atlantic International (Bole), and Xpress Money.

Since June 2009, CBE has been in operation and has opened four branches in South Sudan. CBE has dependable and established connections with numerous globally recognized banks across the globe.

1.3 Statement of the Problem

Cyber security risk management is an ongoing process of identifying, analyzing, evaluating, and addressing your organization's cyber security threats. Cyber security risk management is not simply the job of the security team; everyone in the organization has a role to play (NIST, 2020). Commercial banks of Ethiopia implemented cyber security risk management in order to ensure the most critical threats handled in a timely manner. However, it needs to assess the existing cyber security risk management practices to evaluate the organizations existing security posture and security framework. The cyber security environment of Ethiopian banks faces data breaches, phishing attacks, malware, insider threat, third party risks, regulatory compliance mobile banking risks, emerging technologies and cyber-security skill gaps. This assessment will provide as an input to effectively identify, mitigate and manage cyber security risks in today digital landscapes. Cyber security risks continue to evolve and become more sophisticated so it is necessary to regularly asses their cyber security risk management practices to ensure effectiveness and resilience (ENISA, 2020).

In addition, this assessment aims to identify human factors, asses the resilience of existing Controls, and propose improvements to enhance overall cyber security posture. According to the report of the bank in the cyber risk document registered Commercial Bank of Ethiopia face nearly 28,000 cyber-attack attempts, since 2022 Commercial Bank of Ethiopia. (2024, June 17). Not to mention a system glitch caused by a system upgrade on March 15 2024 that created 490000 legal and illegal transactions total of estimated 802 million birr. That made the bank to totally shutdown the system for half a day to investigate the cause and take corrective actions, Therefore, this paper proposed to assess the existing cyber security risk management practices of Commercial bank of Ethiopia in order to see the gap, evaluate the impact of human factors on effectiveness and asses challenges in their practice to fill it with appropriate solutions.

1.4 Basic Research Questions

This Project work will answer the following three basic questions.

1. What does the practice of cyber security risk management look like in CBE?
2. What is the relationship between human factors and effectiveness of cyber security risk management practices in CBE?
3. What are the challenges CBE facing during implementation of cyber security risk management practices

1.5 Objectives of the Study

1.5.1 General Objective of the Study

The general objective of the study is to assess Cyber security risk management practices and challenges of Commercial bank of Ethiopia

1.5.2 Specific Objective of the Study

Specific objectives of the study will include the following issues:

1. To assess cyber security risk management practices of CBE.
2. To assess the human factors that affect effectiveness of cyber security risk management of CBE
3. To assess the challenges of cyber security risk management practice of CBE

1.6 Significance of the Study

The banking industry plays a pivotal role in economic stability. Effective cyber security risk management is essential for safeguarding financial assets, preventing fraud, and maintaining confidence in the banking system. Trust is paramount in banking. Cyber security breaches can erode customer trust, leading to reputational damage and loss of business. Studying risk management helps banks protect customer data, transactions, and privacy, fostering trust and loyalty. The banking sector is subject to stringent regulatory requirements concerning data protection, privacy, and cyber security. Studying risk management practices ensures compliance with regulations such as GDPR, PCI DSS, and Basel III, reducing legal and financial risks. Banks rely heavily on digital infrastructure for day-to-day operations. Effective risk management ensures operational resilience, enabling banks to withstand cyber-attacks, disruptions, and system failures without compromising services. Cyber security risk management helps banks

detect and prevent various forms of fraud, including unauthorized access, identity theft, phishing, and payment fraud. Proactive risk assessment and mitigation strategies mitigate financial losses and protect customers.(Smith, 2020, p. 75)

The findings of this research will mainly be used by Ethiopian bank industry that will inform them in developing and implementing more robust cyber security framework and to strength their cyber security policy and regulations in addition, to pave a way for other researchers.

1.7 Scope of the study

Cyber security risk management typically involves risk identification, risk assessment, risk mitigation, incident detection and response, continuous monitoring and improvement and compliance and reporting.

Geographical scope

This study focus on analyzing cyber security risk management factors and challenges within infrastructure of commercial bank of Ethiopia head quarter IS security division because this division is the main Information processing of almost most critical operation related with IS security are created implemented and monitored. By focusing in this area, the study aims to provide insights in to the diverse cyber security challenges faced by commercial bank Ethiopia across different operational area. While the selected area offers valuable insights, the study acknowledges limitations related to data availability, risk of confidentiality. Efforts will be made to mitigate these limitations through robust data collection methodologies and using confidential available information.

Temporal scope

This study examines cyber security risk management factors and challenges of commercial bank of Ethiopia over the past three years. By focusing on the past three years, the assessment captures recent development trends, and incidents relevant to cyber security risk management within commercial bank of Ethiopia. The three-year timeframe aligns with typical strategic planning cycle of banking sector. The selected scope strikes a balance between capturing recent developments and providing a sufficient historical context for assessing the effectiveness of cyber security risk management practices within commercial bank, by focusing on these three years the assessment aims to offer actionable insights to support ongoing improvement efforts.

While this scope provides insights into recent trends and developments, it may limit the assessment’s ability to evaluate long-term effectiveness of CSRM practices. Efforts will be made

to address these limitations by conducting robust trend analysis and benchmarking against industry best practices within the defined scope. The effectiveness and challenges of implementing Cyber security risk management practices include factors like technological infrastructure and investment, regulatory environments, human factors, organizational culture and leadership, external threat landscapes, third-party relationships, incident response and resilience, and data protection and privacy. This variable can group in to five domains on their nature and relevance to cyber security risk management. These are technological infrastructure factors, human factors, regulatory compliance, organizational culture and leadership and incident response and resilience factors.

These five domains also categorized into technical and non-technical variables based on their relevance to technology and their implications for the study context. Technical variables include technological factors, regulatory compliance and incident response and resilience factors the non-technical factors are human factors and organizational culture and leadership (Sekaran and Bougie (2016)).

This study will focus only on non-technical factors, which are the most; critical factors the bank facing in recent in cyber security risk management area. While technical factors primarily involve the tools, systems, and technologies used to implement cyber security measures, non-technical factors encompass the human and organizational aspects that influence the effectiveness of these measures.

Methodological scope

This study will use descriptive research design and inferential research design intended to adopt integrated approach combines both quantitative analysis that includes KPIs, survey, questionnaires, and qualitative analysis that includes interviews, focus groups, and document analysis, which includes reviewing internal documents reports, polices and incident logs. Additionally, historical trend analysis will be conducted on historical data of cyber security incidents, breaches and regulatory changes.

1.8 Organization of the Study

The first chapter contains Introduction parts, which includes Background of the study, Background of the organization, statement of the problem, research questions, objectives, the significance and scope of the study. The second chapter contains literature review, studies conducted by different researchers, existing literature on cyber security risk management practices, effectiveness, and challenges and explore relevant theoretical frameworks and models for assessing cyber security risk management and Identify gaps in the literature that the study aims to address.

The third chapter present the research methodology, description of the study area, research Design and Approach, Population, Sampling strategy and Sampling Technique and explain criteria for selecting participants, Data types, sources and detail data collection methods, Research Materials, Methods of data analysis, how data will be analyzed in order to answer research questions, Validity and Reliability and Ethical Considerations. Describe the research approach (e.g., qualitative, quantitative, mixed-methods). The fourth chapter Conceptual Framework that presents a conceptual framework that outlines key factors influencing cyber security risk management effectiveness and challenges.

The fifth chapter contains results, presentation, analysis, interpretation, and conclusion. The last chapter will include summary, conclusion, and recommendation. Finally, references and appendices will be included.

1.9 Definition of terms

Assessment: A process of evaluating the feasibility of project based on predetermined criteria and objectives (Turneret al., 2019).

Cyber security: The practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, and data breaches." (Source: National Institute of Standards and Technology, "Cyber security Framework," 2014)

Cyber security risk:"The potential for harm, loss, or disruption to occur as a result of vulnerabilities or threats targeting an organization's digital assets." (Source: National Cyber Security Centre, "Introduction to Risk Management," 2021)

Risk management: The process of identifying, assessing, and mitigating risks to an organization's assets, including information technology systems and data, in order to reduce the likelihood and impact of security incidents. (Source: International Organization for Standardization, ISO/IEC 27005:2018)
Cyber security risk management:

Practice: The implementation or execution of established procedures, policies, or actions aimed at managing cyber security risks within an organization. (Source: NIST, "Framework for Improving Critical Infrastructure Cyber security," 2018)

Challenges: Factors or obstacles that hinder or impede the effective management of cyber security risks, including technological, organizational, regulatory, or human-related issues.
(Source: NIST, "Special Publication 800-30: Guide for Conducting Risk Assessments," 2012

Chapter Two

Literature Review

2.1 Introduction

The purpose of incorporating theoretical literature in the assessment of cyber security risk management practices and effectiveness, and the identification of challenges within Commercial bank of Ethiopia, serves multiple key functions: provides a foundational framework that underpins the study, offering established theories and models that can explain the phenomena being studied. For cyber security risk management, theories from fields such as information security, organizational behavior, and risk management lay the groundwork for understanding the complex dynamics involved in protecting an organization's digital assets. It offers a rich contextual background that helps to situate the current study within the broader academic and practical discourse on cyber security risk management. This includes insights into how cyber security challenges have evolved, how they are being addressed across the banking industry, and emerging trends that could affect future risk management strategies.

In addition, informs the development of hypotheses or research questions. By understanding the theories and findings from previous research, the assessment can formulate targeted questions that address specific aspects of cyber security risk management practices, their effectiveness, and challenges within CBE.

It enables a comparative analysis of CBE's practices against established theories and models. This comparison can reveal gaps, strengths, and opportunities for improvement in the bank's approach to managing cyber security risks. Evidence-based Recommendations: By grounding the study in theoretical literature, the assessment can make evidence-based recommendations that are supported by well-established theories and research findings. This increases the credibility and relevance of the recommendations for enhancing cyber security risk management practices at CBE.

Theoretical literature helps bridge the gap between academic research and practical application. By aligning the study's findings with theoretical insights, the assessment can contribute to both scholarly discourse and practical improvements in cyber security risk management within the banking sector.

2.2 Theoretical Literature Review

2.2.1 Definition of Risk

The simplest definition of risk is the potential for loss. There could be monetary loss or harm to one's reputation or image (Sharma, 2003)

Risk is the potential for harm and unfavorable, unforeseen events to transpire (Oxford English Dictionary, 2013). Risk is typically used to describe a negative divergence from the plan in economic writings (Maylor, 2010). According to Ghosh (2015), risk in banks is the possibility of suffering a loss as a result of unfavorable circumstances such economic downturns, negative adjustments to trade and fiscal policies, unfavorable changes in interest rates or foreign exchange rates, or falling stock prices. Every firm has risks; some are uncontrollable and unexpected, while others are predictable and under management's authority. We have the ability to take risks in order to increase our returns because higher risks are associated with higher returns (Mehmood, and Zhang, 2010).

Osborne (2012) has indicated that "Risks can arise as a result of our business's activities or as a result of external factors such as legislation, market forces, and interest or exchange rate fluctuations, the activities of others or even the weather. They can be a product of the business environment, the natural environment, and the political or economic climate or of human inadequacies, failures, or errors. The bottom line is that risk may impact on our ability to meet our business objectives or even threaten the business itself."

Risk is the deviation from the expected outcome. In one way, risk classified as business and financial risks. Business risk arises from the nature of a firm's business, which relates to factors affecting the product market and financial risk arises losses in financial markets due to movements in financial variables (Jorion, 1996).

2.2.1.1 Financial risk

The job of keeping an eye on financial hazards and controlling their effects is known as financial risk management.

It is an application of contemporary financial theory and practice and a sub discipline of the larger field of risk management (Moles, 2016).

Raymond (2012) asserts that financial risk management is the financial industry's quality

assurance. It's a general phrase that can refer to many different types of businesses or objects, but it entails identifying, evaluating, and taking action to lessen or completely eliminate an organizations or person's vulnerability to loss.

Banking serves as a middleman between those who want to save money and those who are looking to raise capital for their businesses. As a result, banks take on a variety of risks, both financial and non-financial, in the course of offering financial services. Additionally, this risk inherent in the provision of their services differs from one product or service to the other (Adarkwa, 2011) various writers have grouped. These risks in different ways to develop the frameworks for their analyses Crouhy et al. (2006) formulate a different classification of risks in banks that encompasses operational risk, business risk, legal risk, reputation risk, strategic risk and cyber security risk.

2.2.1.2 Non-Financial Risk

Banks are accustomed to taking on financial risk and generating profit from it. It is the premise of their business models. However, non-financial risk (NFR), weather related to compliance failures, misconduct, and technology or operational challenges (Kaminski et al, 2016).

The following are non-financial risks:

Operational Risk

Malfunction of the information systems, reporting systems, internal monitoring rules and internal procedures designed to take timely corrective actions, or the compliance with the internal risk policy rules result in operational risks (Bessis, 2010). Moreover, human or technological errors, lack of control to prevent unauthorized or inappropriate transactions, fraud and faulty reporting may lead to further losses caused by internal process, people and operating system (Medova, 2001). The operational risk mostly emerges from the inside activities of bank unlike some other forms of risks like market and credit risk. However, a number of sources of operational risk come from the external environment such as competitive actions, natural disasters (such as floods, earthquakes) and terrorist attacks that are largely unpredictable and uncontrollable by banks (Fayyaz, 2006). According to Basel Committee on Banking Supervision (BCBS) definition, there are four causes of operational risk, which are Process, people, and system or external events.

I. Process risks: -inefficiencies or ineffectiveness in the various business processes within the firm. These include value-driving processes, such as sales and

marketing, product development, and customer support, as well as value-supporting processes such as IT, HR, and operations.

II. People risks: - employee error, employee misdeeds, employee unavailability, and inadequate employee development and recruitment.

III. Technology (or system) risks: -As the system, failures caused by breakdown, data quality and integrity issues, inadequate capacity, and poor project management.

Strategic Risk

One of the most significant hazards associated with banking operations is this one, which is linked to strategy choices that affect all other risks (Bessis, 2002). "The risk of significant investments for which there is a high uncertainty about success and profitability" is how Crouhy et al. (2006) describe strategic risk. For example, more competition would force a bank to lend to newly form subprime borrowers with bad credit, while an abrupt rise in interest rates would cause banks' mortgage volume to drop quickly. Potential losses resulting from strategic decisions made by upper management are referred to as strategic risk (Tyrell, 2008). One potential cause of loss that could result from pursuing a failed business plan is strategic risk.

For instance, poor decision-making, poor decision-execution, insufficient resource allocation, or a lack of responsiveness to changes in the business environment can all lead to strategic risk (Bussiness, 2014). Strategic risk is the range of outside events and trends that have the potential to completely destroy a company's growth trajectory and shareholder value, according to Slywotzky and Drzik (2005). While these two authors view strategic risk as the exclusive result of external events, other authors define strategic risk as the present and potential effects on capital and/or earnings resulting from 15 internal business activities, such as poor decision-making, poor execution of decisions, or a failure to adapt to changes in the industry.

They therefore consider strategic risk as a function of the compatibility of an organization’s strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation.

According to Emblemshag and Kjolstad (2002), strategic risk also refers to risk that develops when a company pursues its goals by minimizing dangers or taking advantage of opportunities. In any case, strategic risk includes a wide range of uncertainties that are not financial in nature but rather credit- or operational-related. These uncertainties can be brought about by macroeconomic variables, industry trends, or errors in a firm's strategic decision-making that

have a negative impact on the firm's earnings and shareholders' value. Since they frequently represent some of a company's largest exposures, strategic risks have the potential to seriously undermine value. Slywotzky and Drzik (2005) made an effort to pinpoint important occurrences that raise strategic risk and divided them into seven major groups.

These include industry margin squeeze, threat of technology shift, which has the possibility of driving some products and services out of the market, brand erosion, emergence of one-of-a-kind competitor to seize the lion share of value in the market, customer priority shift, and new project failure and market stagnation. The idea was to provide a framework for assessing a company's strategic risks and develop counter measures to address them. The authors intimate that the key to surviving strategic risks is; knowing how to assess and respond to them and therefore devoting resources to it. They also advice management to adjust their capital allocation decisions by applying a higher cost of capital to riskier projects and to build greater flexibility into their capital structure when faced with riskier competitive environments. The organization's internal characteristics must evaluate against the impact of economic, technological, competitive, regulatory, and other environmental changes. An effective strategic risk management approach should embrace both the upside and downside of risk. It should seek to counter all losses, both from accidents and from unfortunate business judgments, and seize opportunities for gains through organizational innovation and growth. Seizing upside risk involves searching for opportunities and developing plans to act on these opportunities when the future presents them. Countering downside risk on the other hand is done by reducing the 16 possibility of occurring (probability) and scope (magnitude) of losses; and financing recovery from these losses (Herman and Head, 2002)

Reputation Risk

Exposure to damages resulting from damage to one's reputation is known as reputational risk. The institution's apparent ineptitude, carelessness, or wrongdoing may be the cause of its damaged reputation (Tyrell, 2008). Reputation risk, according to Basel (2009), is the potential for losses resulting from a bad opinion held by clients, depositors, rival businesses, market analysts, investors, shareholders, regulators, and other relevant parties. This risk may negatively affect banks' capacity to grow new business ventures or maintain ongoing operations in order to preserve a steady stream of capital (Ishfaq, 2006).

Cyber security risk

Regarding security, there are a minimum of three linked ideas. Cybersecurity, information security, and computer security are these. Information communication, or ICT, security, is defined by Solms and Niekerk (2013) as the safety of computers used for information processing and storage (As Cited in Horne, Ahmed and Maynard, 2016, p. 4). According to the same author, information resources' confidentiality, integrity, availability, non-repudiation, accountability, validity, and dependability are the main objectives of computer security. 14 | P A G E Protecting data and information systems against illegal access, use, disclosure, interruption, or destruction is the second idea of security, or information security. Preserving the confidentiality, integrity, and availability of business information is the aim of information security, according to Mcumber (1991) and Solms (1998). As Cited in Horne, Ahmed and Maynard, 2016, p4),Solms (1998) further stress that information security needs to safeguard business continuity and reduce business impairment by constraining the effect of security incidents (As Cited in Horne, Ahmed and Maynard, 2016, p4). The International Telecommunication Union /ITU/ defines cyber security as follows: Solms (1998) emphasizes further that information security must limit the impact of security incidents in order to protect business continuity and minimize business harm (As Cited in Horne, Ahmed and Maynard, 2016, p. 4). Cyber security is defined by the International Telecommunication Union, or ITU, as follows:
In order to protect the cyber environment, company, and user assets, a variety of tools, policies, security concepts, security safeguards, guidelines, risk management techniques, activities, training, best practices, assurances, and technology are together referred to as cyber security. Assets belonging to organizations and users include networked computers, employees, telecommunications systems, infrastructure, applications, services, and all data that is transferred and/or stored in the cyber environment.
The goal of cyber security is to protect user assets and organizational security properties from pertinent security threats in the online environment. Among the overall goals are the following: • Accessibility • Integrity, which can be defined as non-repudiation and genuineness • Private Information (ITU, 2008) (As cited on page two in Solms and Niekerk, 2013)

Cyber Security Threat Actors

Any type of cyber security breach has the potential to spread, whether on purpose or accidentally. Threat actors include hackers, people connected to the state, company insiders, and malevolent users. According to Sahare, Naik, and Khandey (2014), hacking is the act of taking advantage of a system's vulnerability for one's own gain or satisfaction (p. 1). This is what hackers do. They are referred to as attackers, intruders, or crackers. They have a variety of reasons for hacking. According to the same writers, some hackers hack for enjoyment, some for financial gain, and some just want to mess with your stuff and maybe get noticed. According to the hues or tones of the "Hat," hacking is divided into three categories.

The word "hat" originated in classic western films, where the villains' cap was black and the hero's wore white. It was stated that there is less of a purpose to cause harm the lighter the hue (Sahare, Naik and Khandey, 2014, p.1). The writers divided hackers into three categories—Black Hat Hackers, White Hat Hackers, and Gray Hat Hackers—based on these tenets. IT experts, who are ethically and with good intentions, are approved and compensated by organizations as white hat hackers. To evaluate its security, several businesses hire IT specialists to try to hack their own computers and servers. White hat hackers are sometimes referred to as ethical hackers because they breach security to test their own security framework.

On the other hand, black hat hackers aim to damage networks and computer systems. These types of hackers breach security and enter the network with the intention of damaging or erasing data in order to render the network inoperable. In addition, they violate security, steal data, and deface websites. Similar to inheritance, which allows a derived class to inherit all or some of the properties of the base class or classes, gray hat hackers also inherit the attributes of white hat and black hat hackers. These hackers might have the solution. Although they are fully conscious of right and evil, they occasionally behave negatively (Sahare, NaikandKhandey, 2014, p).

Kosina(2012). Apart from hackers, cybercrime and cyber breaches are also sustained by organized crime groups, the state, and proxies with ties to the state. According to Broadhurst et al. (2014), a lot of governments, or their proxies, are employing internet technology these days to perpetrate crimes. The same authors went on to say that revelations from Edward Snowden about the United States government's extensive cyber surveillance programs matched accusations that China authorities were involved in widespread economic and industrial espionage and that

Russia had carried out or encouraged distributed denial of service attacks.

Furthermore, 'traditional' organized criminal groups may have gotten more active in digital crime, according to conjecture from governments, law enforcement agencies, academic researchers, and the cyber security sector (Broadhurst et al., 2014, p. 3). According to Mc Guire's (2012) assessment, which was based on a sizable sample of documented cases, organized activity, may be the cause of up to 80% of cybercrimes (as referenced by Broadhurst et al., 2014, p. 3). According to Broadhurst et al. (2014), extremist and insurgent groups have been utilizing internet technology as a tool for stealing to increase their base of resources in recent years. According to Sipress (2004), Imam Samudra, the man responsible for the 2002 Bali bombing and now convicted architect, allegedly encouraged his adherents to steal credit cards in order to fund militant activities (As cited Broadhurst et al., 2014, p.3).

Methods of Cyber Attack

The objective of the attacker determines the various shapes that a cyber attack can take. Social engineering, distributed denial-of-service (DDoS), DoS, and malicious code are a few of the techniques that attackers are known to use. We go over each of these cyber attack techniques below.

Social Engineering

Social engineering, commonly referred to as human hacking, is the practice of deceiving clients and staff into divulging login credentials so that you can use them to gain access to accounts or networks, according to Conteh and Schimick (2016) (p. 1). The same authors went on to say that social engineering is a methodology that uses methods to obtain private and confidential information by taking advantage of cognitive biases, which are errors in human reasoning (p. 2). This plan makes advantage of deceit, curiosity, and inner human nature. The same writers went on to say that it is a hacker's cunning use of deceit or manipulation of people's propensity for trust, corporatism, or just following their interest and curiosity. Stated differently, social engineering is a strategy used by attackers to leverage insiders and information in order to utilize deception to get around computer security systems (Conteh and Schimick, 2016 p.2). Notwithstanding advancements in technology, human error remains an unavoidable aspect in

cyber security breaches. Because of this, Conteh and Schimick (2016) said that although security measures are meant to strengthen the security of information systems, human factors are a weak point that can be exploited in a social engineering attack (p. 2). Five of the most typical forms of social engineering attack victims are identified by Bisson (2015), who also points out that social engineering, cover a wide range of malicious activities. These victims include 20 | P a g e phishing, pre-texting, baiting, Quid pro quo, and tailgating (Conteh and Schimick, 2016, p.2). Conteh and Schimick (2016) describe phishing frauds as an attempt to obtain personal information such as names, address and other personal identifiable information such as social security numbers. Phishing scammers may include links in their emails that take victims to dubious-looking but authentic websites. It also launches attacks using email services. Phishing scams, a form of social engineering, instill a sense of urgency in its victims so they will act against their better judgment (p. 4). The second sort of social engineering, called pre-texting, is explained by the same authors. It involves a fabrication scenario aimed at verifying and obtaining personal information from a target. With this technique, the attacker must create a convincing narrative that the target finds difficult to refute. The tactic aims to establish a sense of trust with the victim by instilling anxiety and urgency in order to confirm or collect the desired information (p. 4). Phishing attacks and baiting are comparable. Hackers utilize the promise of products in exchange for a user giving up their login information to a particular website. Quid pro quo, which is comparable to baiting, involves an attacker posing as an IT representative and helping victims who could be having technical difficulties. In the last social engineering approach, the attacker leverages piggy backing and tailgating to obtain access to regions that are banned. According to Conteh and Schimick (2016), p. 4, this attack exposes those who have the capacity to grant or gain access to a restricted location by an attacker posing as delivery persons or other people who might need temporary access.

Denial-of-Service /DoS/

Denial-of-Service (DOS) attacks are described by Kosina (2012) as an effort to prevent authorized users from accessing an online resource, usually a website (P. 16). This attack technique sends out a continuous stream of server requests. According to the same author, DOS assaults operate by "flooding" the resource with a lot of requests. The author went on to detail the impact of the assault, stating that it overwhelms the server to the point where it can no longer handle all of the requests (Kosina, 2012, P. 16). According to Luo, Chang, and Chan (2005),

denial-of-service (DOS) attacks are among the worst because they drain resources such as compute cycles, buffers, and communication bandwidth, which has an impact on computer and communication performance 21 | P a g e (As Cited by Chee-Wooi Ten, 2010.p.3).

However, the attacker will not be able to achieve the desired outcome for this assault with a single computer or small number of computers. Because it is simple to stop the DOS attack's original source. As such, Distributed-Denial-of-Service, or DDOS, attacks account for the majority of DOS attacks. DDoS attacks can be carried out by having computer users willingly band together to take part in the attack, according to Kosina (2012). According to the author, denial-of-service assaults (DDOS) are typically carried out through botnets, which are networks of compromised computers whose owners are unaware that their workstations are under attack. Installing malicious software, also known as malware, on the computer enables a third party—the real attacker—to seize control of it and transform it into a bot—short for robot—that takes part in the denial-of-service attack (Kosina, 2012, P.17). The same author further stated that a Denial-of-Service attack is among the widest spread cyber-attacks.

Website Defacement

Website defacement, according to Kosina (2012), is an attack on a website that modifies the content of that website. According to Kosina (2012), P. 18, the updated content mocks the target or expresses the attacker's political or ideological beliefs, reflecting their intent. The same blogger went on to say that one of the most popular techniques for defacing websites is SQL injection, which is essentially a way to send commands to a database by inputting malicious data into a web form.

Malicious Code

Programming code that can compromise a computer system's availability, data integrity, or secrecy is known as malicious code; this category includes Trojan horses, malware, viruses, worms, and trapdoors (Dictionary of computing and communications, 2003). These harmful software have the ability to replicate and spread throughout a computer network. They can also be transferred via flash drives from one computer to another and via internal user devices (Bring your own devices, or BYOD).

2.2.2 Risk management

Risk management is a fundamental process for organizations to navigate uncertainties and mitigate potential threats to their objectives, resources, and stakeholders. This literature review synthesizes key concepts, theoretical frameworks, best practices, and empirical research in the field of risk management.

Risk management involves several key concepts, beginning with risk identification, where organizations systematically identify and characterize potential risks that could affect their operations (Hillson& Murray, 2017). Subsequently, risk assessment evaluates the likelihood and potential impact of identified risks, enabling organizations to prioritize them for mitigation efforts (Fraser &Simkins, 2010). Risk mitigation strategies aim to reduce the probability and severity of adverse events, utilizing techniques such as risk avoidance, risk reduction, risk transfer, and risk acceptance (Hillson& Murray, 2017).

Theoretical Frameworks in Risk Management

Theoretical frameworks provide structure and guidance for effective risk management practices. The ISO 31000:2018 standard offers a comprehensive approach to risk management, emphasizing principles such as risk-based decision-making, integration with organizational processes, and continual improvement (ISO, 2018). Similarly, the COSO Enterprise Risk Management Framework emphasizes the importance of aligning risk management with an organization's strategic objectives, values, and culture (COSO, 2017).

Best Practices in Risk Management

Best practices in risk management encompass a range of strategies and techniques to identify, assess, and mitigate risks effectively. Risk registers and risk matrices are commonly used tools to document and prioritize risks based on their likelihood and impact (Hull, 2018). Additionally, organizations often employ scenario analysis and stress testing to evaluate the potential consequences of adverse events and enhance preparedness (Fraser &Simkins, 2010).

Types of risk management

I. Financial Risk Management:

Financial risk management involves identifying, assessing, and mitigating risks related to financial instruments, markets, and investments. It encompasses market risk, credit risk, liquidity risk, and operational risk within financial institutions (Hull, 2018).

II. Operational Risk Management:

Operational risk management focuses on identifying, assessing, and managing risks arising from internal processes, people, systems, and external events that could disrupt business operations or cause financial losses. It includes risks related to technology, human error, fraud, and legal compliance (Lam, 2003).

Strategic Risk Management:

Strategic risk management involves identifying and addressing risks associated with strategic decisions and objectives. It encompasses risks related to market competition, technological changes, regulatory shifts, and geopolitical factors that could affect the organization's long-term success (Fraser &Simkins, 2010).

III. Compliance Risk Management:

Compliance risk management focuses on ensuring that organizations adhere to relevant laws, regulations, and industry standards. It involves identifying regulatory requirements, assessing compliance gaps, and implementing controls to mitigate the risk of non-compliance and potential legal penalties (Peltier, 2016).

IV. Reputational Risk Management:

Reputational risk management involves protecting and enhancing an organization's reputation by identifying and mitigating risks that could damage its brand, public perception, or stakeholder trust. It includes risks related to ethical breaches, negative publicity, and customer dissatisfaction (Lindgreen et al., 2012).

V. Cyber security Risk Management:

Cyber security risk management focuses on identifying, assessing, and mitigating risks related to information security threats and vulnerabilities. It includes risks such as data breaches, malware attacks, phishing attempts, and insider threats (Schneier, 2019).

2.2.3 Cyber security Risk Management Practices in Banking

Cyber security risk management in banking is a multifaceted process aimed at identifying, assessing, mitigating, and monitoring cyber threats and vulnerabilities to protect sensitive financial data and maintain the integrity of banking operations. Drawing upon established risk

management frameworks and best practices, banking institutions employ a range of strategies and techniques for managing effectively cyber security risks. These are:

Risk Assessment and Identification

One of the foundational elements of cyber security risk management in banking is the thorough assessment and identification of potential risks and vulnerabilities. This process involves conducting comprehensive risk assessments to identify and prioritize cyber threats, assess the likelihood and potential impact of security incidents, and evaluate existing control measures. According to the Risk Management Framework (RMF) outlined by the National Institute of Standards and Technology (NIST), risk assessment in banking encompasses the identification of assets, threats, vulnerabilities, and potential impacts, leading to the development of risk mitigation strategies (NIST, 2020).

Risk Mitigation and Controls Implementation

Once risks identified and assessed, banking institutions implement a variety of risk mitigation strategies and control measures to reduce the likelihood and impact of cyber threats. This includes the implementation of technical controls such as firewalls, intrusion detection systems, encryption protocols, and multi-factor authentication to safeguard sensitive data and systems from unauthorized access and malicious activities. Additionally, banks enforce strict access controls, regularly patch and update software and systems, and conduct security awareness training for employees to mitigate the risk of insider threats and human errors (Choi et al., 2019).

Continuous Monitoring and Response

Cyber security risk management in banking is an ongoing process that requires continuous monitoring and proactive response to emerging threats and vulnerabilities. Banking institutions leverage advanced security monitoring tools and technologies to detect and analyze potential security incidents in real-time, enabling rapid response and containment efforts. Incident response plans and procedures established to facilitate coordinated responses to cyber incidents, minimize disruption to banking operations, and mitigate the financial and reputational impacts of security breaches (Kannan et al., 2021).

In conclusion, effective cyber security risk management practices in banking involve a systematic approach to identifying, assessing, mitigating, and monitoring cyber risks. By employing robust risk assessment methodologies, implementing appropriate control measures,

and maintaining vigilance through continuous monitoring and response efforts, banking institutions can enhance their resilience against cyber threats and safeguard the integrity of financial systems and customer data.

The cyber security risk management practices also include

Employee Training and Awareness Programs:

Banks invest in comprehensive employee training and awareness programs to educate staff members about cyber security best practices, policies, and procedures. Regular training sessions and simulated phishing exercises help employees recognize and respond to potential threats, reducing the risk of human error and insider threats (Johnson & White, 2020).

Vendor Risk Management:

Given the interconnected nature of the financial ecosystem, banks often rely on third-party vendors and service providers for various functions. Effective vendor- risk management practices involve assessing and monitoring the cyber security posture of vendors, establishing contractual requirements for security controls, and conducting regular audits to ensure compliance with regulatory standards (Roberts et al., 2019).

Regulatory Compliance and Governance:

Compliance with regulatory requirements is a cornerstone of cyber security risk management in banking. Banks adhere to industry-specific regulations such as the Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR), as well as sector-specific guidelines issued by regulatory authorities (Smith & Brown, 2021).

Cyber Threat Intelligence Sharing:

Banks participate in cyber threat intelligence sharing initiatives to exchange information about emerging threats, attack patterns, and vulnerabilities with industry peers, government agencies, and security organizations. Collaborative efforts enhance situational awareness and enable banks proactively defend against cyber-attacks (Davis et al., 2020).

Encryption and Data Protection:

Banks employ encryption techniques to protect sensitive data both in transit and at rest. Encryption ensures that data securely transmitted over networks and stored in databases,

reducing the risk of unauthorized access or interception by malicious actors (Chen & Lee, 2018).

Cyber Security Governance Structure:

Establishing a robust cyber-security governance structure is essential for effective risk management in banking. This involves defining roles and responsibilities for cyber security oversight, establishing reporting mechanisms to senior management and the board of directors, and integrating cyber security considerations into the overall enterprise -risk management framework (Jackson et al., 2020).

Cyber Security Incident Response Exercises:

Regular Cyber security incident response include such as tabletop simulations and scenario-based drills, enable banks to test the effectiveness of their incident response plans and procedures. These exercises help identify gaps in response capabilities, improve coordination among internal and external stakeholders, and enhance the bank's preparedness to respond to cyber security incidents (Gonzalez & Martinez, 2019).

Security Information Sharing Platforms:

Banks participate in security information sharing platforms and forums where they can exchange threat intelligence, indicators of compromise (IOCs), and best practices with other financial institutions and security organizations. Collaborative sharing of information enhances the industry's collective defense against cyber threats and facilitates faster detection and response to emerging threats (Wang & Liu, 2021).

Secure Software Development Lifecycle (SDLC):

Banks implement secure software development practices to ensure that applications and systems developed with security in mind from the outset. This involves integrating security controls and best practices throughout the software development lifecycle, including requirements gathering, design, coding, testing, deployment, and maintenance (Khan & Ahmed, 2020).

In conclusion, cyber security risk management in banking requires a multifaceted approach that encompasses technical, organizational, and collaborative strategies. By implementing encryption and data protection measures, establishing a robust governance structure, conducting incident response exercises, and participating in security information sharing initiatives, banks can enhance their resilience to cyber threats and maintain the trust and confidence of their customers.

2.2.6 Challenges of cyber security risk management practices

Despite the implementation of various cyber security risk management practices, banks face several challenges that can impede their effectiveness in mitigating cyber threats. This section examines some of the key challenges encountered by banks in managing cyber security risks.

1. Rapidly Evolving Threat Landscape:

One of the primary challenges faced by banks is the rapidly evolving nature of cyber threats. Cyber adversaries continuously develop new tactics, techniques, and procedures (TTPs) to exploit vulnerabilities and circumvent security controls. Keeping pace with these evolving threats requires banks to continually update their defenses and invest in advanced threat intelligence capabilities (Smith & Johnson, 2020).

2. Insider Threats and Human Error:

Insider threats, whether intentional or unintentional, pose significant risks to banks' cyber security. Employees, contractors, or third-party vendors with privileged access to systems and data inadvertently or maliciously compromise security controls, leading to data breaches or other security incidents. Addressing insider threats requires a combination of technical controls, employee training, and robust access management policies (Brown et al., 2019).

3. Complexity of Information Technology Infrastructure:

The complexity of banks' IT infrastructure, including legacy systems, interconnected networks, and third-party integrations, presents challenges for cyber security risk management. Legacy systems may lack modern security features, be more vulnerable to exploitation, while interconnected networks increase the attack surface, and complicate threat detection and response. Banks must carefully manage and secure their IT assets while modernizing legacy systems to address security vulnerabilities (Garcia & Patel, 2018).

4. Compliance with Regulatory Requirements:

Banks operate in a highly regulated environment, with numerous regulatory requirements and industry standards governing cyber security practices. Achieving compliance with regulations such as the Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), and the General Data Protection Regulation (GDPR) can be challenging due to the complexity and evolving nature of regulatory frameworks. Banks must allocate resources and implement controls to ensure compliance while balancing regulatory requirements

with operational needs (Jones & Smith, 2021).

6. Resource Constraints:

Resource constraints, including budgetary limitations and staffing shortages, pose significant challenges for banks in implementing effective cyber security risk management practices. Limited resources may hinder banks' ability to invest in advanced security technologies, conduct regular security assessments, and hire skilled cyber security professionals, leaving them vulnerable to cyber-attacks (Clark & Robinson, 2019).

7. Third-Party Risk Management:

Banks rely on third-party vendors and service providers for various functions, including cloud services, payment processing, and data analytics. Managing third-party cyber security risks presents challenges related to assessing the security posture of vendors, enforcing contractual agreements, and ensuring compliance with regulatory requirements. Failure of effectively managing third-party risks can expose banks to supply chain attacks and data breaches (Patel & Lee, 2021).

8. Lack of Cyber Security Awareness:

Despite investments in employee training programs, maintaining a strong culture of cyber security awareness remains a challenge for banks. Employees may lack awareness of emerging cyber threats, fail to recognize phishing attempts, or disregard security policies and procedures, increasing the risk of security incidents. Enhancing cyber security awareness among employees requires ongoing education, communication, and reinforcement of security best practices (Garcia & Wang, 2020).

9. Cultural resistance to change

Cultural resistance to change within organizations can hinder the implementation of cyber security risk management practices. Resistance may stem from employee skepticism, reluctance to adopt new technologies or processes, or complacence with existing practices. Overcoming cultural resistance requires effective change management strategies, clear communication, and engagement with stakeholders at all levels of the organization (Wan&Lee, 2021).

Conclusion:

In conclusion, the challenges of cyber security risk management practices in banking underscore the importance of a proactive and adaptive approach to cyber security. By addressing challenges such as the rapidly evolving threat landscape, insider threats, complexity of IT infrastructure and

compliance with regulatory requirements, cultural resistance to change banks can enhance their cyber resilience and effectively mitigate cyber risks. In addition, the challenges of cyber security risk management practices in banking underscore the need for a holistic and proactive approach to cyber security. By addressing challenges such as advanced persistent threats, resource constraints, third-party risk management, and cyber security awareness, banks can strengthen their cyber resilience and effectively mitigate cyber risks in today's evolving threat landscape

2.2.4 Factors affecting effectiveness Cyber security Risk Management Practices in Banking

Cyber security metrics are categorized into technical and non-technical dimensions, providing a structured approach to understanding and measuring cyber security effectiveness. It distinguishes between technical metrics related to IT infrastructure, security tools, and vulnerability management, and non-technical metrics involving human factors, organizational culture, and compliance with regulations. The classification helps in assessing and improving cyber security practices by addressing both technological capabilities and behavioral aspects within organizations Huang, Y., & Nicol, D. M. (2013).

Both technical and non-technical factors play complementary roles in ensuring effective cyber security risk management practices in banking. A holistic approach that addresses these factors in tandem is essential to mitigate cyber threats and protect sensitive financial information and customer data.

Technical Factors in Cyber security

Technological Infrastructure

The strength and resilience of IT infrastructure including networks, servers, and endpoints, are critical for defending against cyber threats (Sood et al., 2013).

Security Technologies

Implementation of advanced security technologies such as intrusion detection/prevention systems (IDS/IPS), firewalls, and endpoint protection platforms (EPP) enhances the ability to detect and respond to threats (Scarfone & Mell, 2007).

Encryption and Data Protection

Uses of encryption protocols and data protection mechanisms: to safeguard sensitive information

from unauthorized access (Boyd et al., 2004).

Patch Management

Timely application of security patches and updates to software and systems to mitigate known vulnerabilities (Shin & Yoo, 2011).

Network Security

Implementation of network segmentation, VPNs (Virtual Private Networks), and strong access controls to prevent unauthorized access and data breaches (CISCO, 2020).

Non- Technical Factors in Cyber security

Human factors in cyber security

Human factors play a crucial role in cyber security, encompassing various aspects such as security awareness and training, behavioral psychology, cognitive load, and social influence, leadership commitment, security culture and communication and collaboration . Here are some insights and citations on each of these factors:

Security Awareness and Training

Security Awareness: Effective security awareness programs enhance employees' understanding of cyber security risks and promote secure behaviors (Herath & Rao, 2009).

Training: Regular training sessions and simulations help employees recognize phishing attempts, understand the importance of strong passwords, and adhere to security policies (Siponen & Vance, 2010).

Behavioral aspect

Understanding human behavior helps in designing security policies that align with employees' motivations and perceptions of risk (Anderson & Agarwal, 2010).

Cognitive Load

Cognitive load theory helps in understanding how the complexity of security tasks impacts users' ability to make secure decisions (Sasse et al., 2001).

Psychological Factors

Risk Perception and Decision Making: Individuals' perception of cyber security risks and their decision-making processes are influenced by psychological factors such as perceived vulnerability and severity of threats (Vance et al., 2012).

Trust and Distrust: Trust in organizational policies and IT systems, as well as distrust due to perceived vulnerabilities or past incidents, affect compliance with security protocols (Riegelsberger et al., 2005).

Social Influence

Social Norms: Workplace norms and peer influence can either reinforce or undermine security behaviors among employees (Choi & Kim, 2010).

Leadership Commitment

Leadership commitment to cyber security sets the tone for the entire organization. When senior executives prioritize cyber security as a strategic priority, allocate resources, and actively participate in security initiatives, it demonstrates the importance of security throughout the organization (Straub et al., 2004).

Security Culture

Security culture refers to the collective attitudes, beliefs, and behaviors related to cyber security within an organization. A strong security culture encourages employees to take responsibility for security, adhere to policies, and remain vigilant against potential threats. It involves fostering awareness, promoting best practices, and integrating security into everyday operations (Hu et al., 2020).

Communication and Collaboration

Effective communication and collaboration between different stakeholders (e.g., IT security teams, management, and employees) are essential for cyber security. Clear and timely communication ensures that security incidents are reported promptly, risks are understood across departments, and security measures are effectively implemented and monitored (Yao et al.,

2019).

From this literature review, there are so many variables be considered in this study. This study focus on the non-technical variables, as mentioned and justified on the scope of study and their overall relationship on the effectiveness of cyber security risk management of CBE

Based on the two domains specified—human factors, organizational culture—we can construct a conceptual framework to this study on assessing the implementation of cyber security risk management practices in CBE.

Human Factors:

This domain encompasses the knowledge, skills, behaviors, and attitudes of individuals within CBE related to cyber security practices.

Variables within this domain may include:

Employee awareness and training: The level of awareness and training provided to employees regarding cyber security risks and best practices.

Behavioral Aspect: Behavioral aspects refer to how individuals within an organization perceive, understand, and act upon cyber security practices and policies (Herath, T., & Rao, H. R. (2009).

Cognitive load: Cognitive load refers to the mental effort required to process information and make decisions. In cyber security, cognitive load impacts: decision making user interface design and training effectiveness (Vance, A., Siponen, M., & Pahnila, S. (2012).

Psychological factors: encompass emotions, attitudes, beliefs, and motivations that influence cyber security behaviors (Lai, V. S., & Li, H. (2005)

Social influence refers to how individuals are influenced by their peers, superiors, and organizational cultures in cyber security contexts are norm, culture and group dynamics (Meske, C., & Stieglitz, S. (2013).

Organizational Culture:

Organizational culture refers to the shared values, beliefs, norms, and practices that shape behavior within CBE with respect to cyber security.

Variables within this domain may include:

Leadership commitment: higher management support and priority for cyber security initiatives

Security culture: The extent to which an organization cultivates a security-conscious culture that encourages shared accountability for cyber security.

Communication and collaboration: effectiveness of communication channels and collaboration mechanisms for sharing cyber security-related information and promoting a culture of security awareness

Organizational culture acts as a mediating variable by shaping employee attitudes, behaviors, and decision-making processes regarding cyber security. It underscores the importance of fostering a culture that values security, promotes accountability, and encourages collaboration across all levels of the organization to effectively mitigate cyber security risks

This conceptual framework outlines the key domains and variables relevant to assessing the implementation of cyber security risk management practices in CBE. By examining these factors, we can gain insights into the organizational dynamics and capabilities that influence the effectiveness of cyber security practices and inform recommendations for improvement.

Relationships:

Human Factors and Effectiveness of Cyber Security Risk Management Practices:

The level of employee awareness, training programs, security behavior, and expertise directly influences the effectiveness of cyber security risk management practices. When employees are well trained and aware of cyber security risks, they are more likely to adhere to security protocols and contribute to a secure environment, thus enhancing the effectiveness of cyber security measures.

Organizational Culture and Effectiveness of Cyber Security Risk Management Practices:

The leadership commitment, communication norms, collaboration culture, and organizational attitudes towards risk and compliance shape the overall organizational approach to cyber security. A positive organizational culture that values and prioritizes cyber security will foster an environment where effective risk management practices are encouraged, implemented, and sustained.

Human Factors and Organizational Culture:

Human factors and organizational culture are intertwined and mutually reinforcing. The effectiveness of employee awareness programs, training initiatives, and security behavior is influenced by the prevailing organizational culture. Similarly, the organizational culture is shaped by the collective attitudes, behaviors, and actions of employees towards cyber security.

2.2.5 Effectiveness of cyber security risk management practices

Measuring the effectiveness of cyber security risk management practices is crucial for organizations to assess their security posture, identify vulnerabilities, and improve resilience against cyber threats. Here are some key aspects and approaches to measuring the effectiveness of cyber security risk management practices:

Risk Identification and Assessment:

Evaluate the organization's ability to identify and assess cyber security risks across its systems, networks, and data assets.

According to NIST, "Risk assessment is the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

Technologies and Controls:

Implementation of technological measures: such as firewalls, intrusion detection/prevention systems (IDS/IPS), encryption, and endpoint protection platforms (EPP) to safeguard bank assets CISCO. (2020).

Third-Party Risk Management

Techniques for managing risks associated with third-party vendors and suppliers, including due diligence, contractual agreements, and continuous monitoring.

"Financial institutions should implement a risk-based approach to managing third-party relationships, which includes conducting due diligence, negotiating contracts that address cyber security requirements, and establishing ongoing monitoring and reporting mechanisms" (Deloitte, 2020).

Emerging Threats and Adaptation:

Strategies for identifying and responding to emerging cyber security threats such as ransom ware, zero-day vulnerabilities, and advanced persistent threats (APTs).

The Cyber security and Infrastructure Security Agency (CISA) provides guidance on emerging

threats and proactive measures for financial institutions.

2.3 Empirical Review of the Literature

The empirical study will elaborate on the relevant previous research that is correlated with the methods used in this research to be used as references to develop the methods and solve the problems in this research.

The empirical literature on cyber security in the banking sector reveals a comprehensive overview of various strategies and their effectiveness, regulatory impacts, and the critical role of awareness and training programs. In their comparative study, Smith & Johnson (2020) in the "Journal of Banking and Finance Security" delve into the effectiveness of cyber security controls within banks. They conclude that advanced cyber security measures significantly lessen the occurrence of cyber-attacks, suggesting a pivotal shift towards more sophisticated security protocols to mitigate threats effectively. This study underscores the importance of adopting cutting-edge cyber security technologies and practices as a crucial line of defense against the increasingly sophisticated landscape of cyber threats faced by banks. They conducted a comparative study to evaluate the effectiveness of cyber security controls in banking. Employing a quantitative approach, they analyzed data from multiple banks to compare the incidence of cyber-attacks with the sophistication of cyber security measures implemented. The study likely utilized a large dataset comprising information from various banks, ensuring a representative sample. However, limitations may arise due to variations in data collection methods or reporting standards among banks, potentially introducing biases or inaccuracies. Additionally, the study may not account for all factors influencing cyber security effectiveness, such as organizational culture or specific threat landscapes faced by individual banks.

Martinez & Garcia (2019), publishing in the "Journal of Financial Regulation," explore the intricate dynamics between regulatory compliance and cyber security practices in the banking sector. They investigated the impact of regulatory compliance on cyber security practices within the banking sector through a case study analysis. Utilizing qualitative methods, they gathered insights from multiple banks to understand the relationship between regulatory compliance and cyber security. The study likely selected a sample of banks from different regions or jurisdictions to capture diverse regulatory environments and cyber security practices. However, case study

analysis may limit generalizability, as findings may not be applicable to all banks or regulatory environments. Additionally, accessing confidential or sensitive information from banks may pose challenges, limiting the depth of analysis. Their research indicates that while regulatory compliance undoubtedly enhances cyber security measures, it may inadvertently stifle innovation by anchoring institutions to specific standards that may not evolve as rapidly as cyber threats do. The implication here is twofold: firstly, regulatory frameworks must be dynamic and adaptive to keep pace with technological advancements; secondly, banks should not solely rely on compliance for security but also pursue innovative cyber security solutions that exceed regulatory requirements.

Furthermore, Brown et al. (2021) in their publication in the "Journal of Cyber Security Research" highlight the indispensable role of cyber security awareness and training programs. Through a series of case studies across various banking institutions, they demonstrate that a well-informed and cyber security-aware workforce significantly bolsters an institution's defense mechanisms against cyber threats. They conducted a case study analysis of cyber security awareness and training programs in banking institutions. Employing a mixed-methods approach, they combined qualitative interviews or surveys with quantitative data analysis to evaluate the effectiveness of training programs. The study likely selected a sample of banking institutions representing various sizes, geographical locations, and cyber-security maturity levels. However, the chosen institutions may not fully represent the broader banking sector, potentially introducing selection bias. Additionally, measuring the long-term impact of training programs on cyber security outcomes may be challenging, as effects may be difficult to quantify or may take time to manifest.

This study brings to light the critical need for ongoing education and training programs tailored to all levels of bank staff, reinforcing the notion that technology alone is insufficient without the support of a vigilant and informed human element.

In summary, while each study offers valuable insights into cyber security risk management practices in the banking sector, they also face methodological limitations. Combining their findings provides a more comprehensive understanding of the challenges and opportunities in bolstering cyber security within banking institutions. However, future research should aim to address these limitations through rigorous methodologies and larger, more diverse samples to ensure robust and generalizable findings

Collectively, these studies offer a nuanced understanding of cyber security risk management in the banking sector, emphasizing a balanced approach that incorporates advanced technological defenses, a forward-thinking stance on regulatory compliance, and a strong organizational culture of cyber security awareness and education. For banks aiming to fortify their cyber security posture, these insights suggest a multifaceted strategy that not only addresses the technological aspects of cyber security but also considers regulatory and human factors as integral components of an effective cyber security framework.

Related Empirical Studies in Ethiopia

The following section will present related studies conducted by different researchers in Ethiopia.

Fekadeselassie (2015) conducted the research on Risk Management Practice of Ethiopian Commercial Banks.

The aim of this paper is to analyze the effectiveness of risk management practice of commercial banks operating in Ethiopia.

The paper's main conclusions are as follows: risk managers believe that risk management is essential to their bank's performance; credit, operational, liquidity, interest rate, and foreign exchange risks are the risks that cause the greatest exposures; current risk management practices have had some success; and banks are using some of the more conventional approaches and techniques to manage risks. Overall, the results imply that Ethiopian banks do, in fact, prioritize risk. A number of recommendations were made, chief among them being that banks should prioritize training their employees in risk management; they should also make risk quantifiable, visible, and manageable; and they should guarantee that there is a significant risk culture across all operations.

Nigussie (2016) assessed determining factors of Best Risk Management Practice based on fifteen commercial banks operating in Ethiopia. For this study, there are six independent variables: understanding risk and risk management (URM), risk assessment and analysis (RAA), risk identification (RI), risk monitoring (RM), Risk Evaluation (RE), and required policy in place (RP) and one dependent variable, RMP. Therefore, regression model applied to analyze the impact of independent variables on dependent variables. From the analysis, it concluded that there were five variables, which have positive significance impact on the dependent variable RMP.

According to Awgchew (2017), the primary goal of this study was to evaluate the problems and practices of private commercial banks in Ethiopia with regard to managing liquidity risk. Fundamental research questions were developed to address the issue of whether or not banks manage liquidity risk in compliance with Basel rules. Additionally, this study examined each bank's performance exposure to liquidity risk. The study's conclusions showed that, when measured against Basel's best practices, Ethiopia's private commercial banks' practices for managing liquidity risk are only partially met. The fundamentals of managing liquidity risk cannot be addressed by centralized, uniform methods of controlling liquidity risk.

According to this survey, the NBE bill purchase policy imposed on private commercial banks, financial innovation and the expansion of global markets, and the growing real-time nature of payment and settlement systems are the key issues faced by the majority of private banks. Additionally, the liquidity position of all private commercial banks has declined annually, and institutions need to make a concerted effort to address this issue. In order to meet their business objectives, the studies concluded by recommending that banks upgrade or improve key components of their liquidity risk management system, diversify their funding sources, and actively monitor their intraday liquidity position.

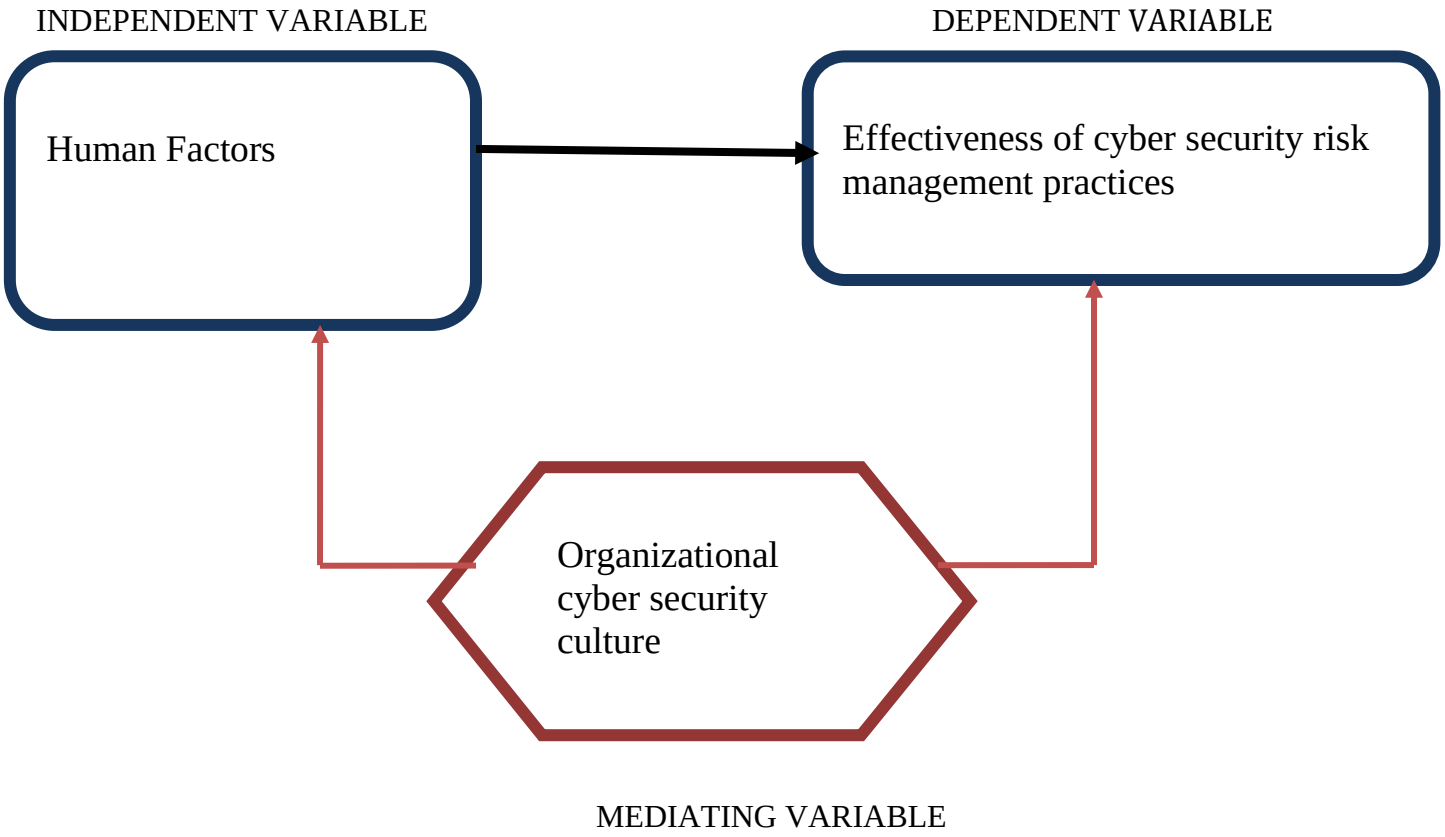
Aragaw (2016) evaluated Ethiopia's commercial banks' credit risk-management practices. Credit risk-management practice was the dependent variable, and the independent variables included creating a suitable environment for credit risk, adhering to a sound credit-granting procedure, keeping up a suitable credit administration, measurement, and monitoring system, and guaranteeing sufficient control over credit risk. The total result demonstrates a strong and positive correlation between the practice of credit risk management and the creation of a suitable environment for credit risk.

In Firew's (2012) study, operational risk indicators were evaluated together with their effect on commercial bank of Ethiopia performance. A mixed study design (qualitative and quantitative) was employed by the researcher. The results demonstrated that operational risk effects, operational risk factors, business disruption, and system failure have a strong and positive relationship with operational risk. Ultimately, the majority of the findings are reported by the researcher.

Summary and Knowledge gap

Few studies have been conducted that offer empirical support for Ethiopian commercial banks' risk management practices. To the best of the researcher's knowledge, no research has been done specifically examining how commercial banks handle cyber security risk; instead, the majority of earlier studies concentrated on financial concerns, such as credit, liquidity, market, and operational risk. Except from reputational, cyber, and strategic risks, operational risk is nonfinancial risk. In theory, banks carry both non-financial and financial risks. This study attempted to close this gap in the literature by concentrating on one of the nonfinancial hazards (cyber risk), which is very dynamic and in need of additional research.

2.4 CONCEPTUAL FRAMEWORK:



Source: Developed by the author based on literature review, 2024

Figure 1 Conceptual framework

Chapter Three

Research Methodology

This part of the research will focus on the research design, research study area, target population, sampling technique, data source and data collection tools and techniques that will be used in this study.

3.1 Description of the study area

This study conducted in Addis Ababa, Commercial bank of Ethiopia Cyber security department. CBE has been applying multiple cyber security risk management practices among those of this study will focus on risk identification and assessment, technology and control, third party risk management and emerging threat adaptations and its challenges.

3.2 Research Design and Approach

This research targeted effectiveness of cyber security risk management practice and challenges. Because the research will answer what questions of the cyber security risk management, it used descriptive research design to assess the practices and challenges of cyber security risk management and inferential analysis (explanatory research design) used to assess how more or less the identified factors affect the CSRMS must be shown by regression analysis.

The research applied both qualitative and quantitative research approach to analyze the data collected. Quantitative research approach used to analyze the data collected through close -ended questions and qualitative research approach used to analyze data collected through open-ended questions and Interviews.

3.3 Target Population, and Sampling

The study target on Cyber security division of Commercial bank of Ethiopia (CBE) located in Addis Ababa. This study only focused on three of these departments: Cyber security operation center IS security implementation and administration and IS Fraud investigation department of cyber security division. On there are 66 employees including the manager for each department.20 from Cyber security operation center department, 22 from IS Security administration and implementation department and the rest 24 are from IS fraud investigation department.

According to the selection of departments the three departments have 66 employees and all of the population taken as a census.

3.4 Data types, sources and methods of data collection

Data types and sources of data

Data required to conduct research can be collected by either using primary or secondary data sources (Catherine, 2007). This study will use both primary and secondary data. Questionnaires that will be prepared and distributed accordingly at cyber security division of CBE will collect primary data. In addition, interview questions will also be used to collect primary data from the following stakeholders: IT security personnel, managements, end-users, and employees. There are also regulatory compliance, audit findings data; training data; risk assessment reports, risk registers, risk management platforms, policy document and procedure manuals found in Bank (CBE)and that will be used as secondary data.

Methods of data collection

Questionnaires that are prepared to collect primary data distributed to the sample unit by their respective email address. Personal (face-to-face) interviews arranged with three managers from department of cyber security department, IS security administration and fraud department among the in order to address critical issues and gather their insights and experiences. The type of interview is going to be Standardized, open-ended interview, because they can be more easily analyzed and compared.

Research Materials

By the time of inconvenience Google forms tool is an open Source online application that is available will be used as survey platform for this study but most the survey will be done one to one in person. The study distributed the questionnaire prepared by using Google form builder via email and responses will automatically be recorded in excel format by this form builder.

3.5 Methods of data analysis

In the study, the data analysis involved analyzing both qualitative and quantitative parts of the data collected. Close-ended questions from questionnaires will be analyzed by quantitative data analysis tools software (SPSS) to perform descriptive statistics,

Descriptive statistics used to summarize the current practices of cyber security risk management within CBE. This could include measures of central tendency, variability, and frequency

distributions to describe key aspects such as the types of security measures employed, the level of employee training and awareness, and the overall organizational culture regarding cyber security.

Both qualitative and quantitative data analysis were used in the study. The Statistical Package for Social Sciences, version 26, was used to do quantitative analysis on closed-ended questions from questionnaires (SPSS V26). The basic or demographic data of the respondents was assessed and described using descriptive statistics like frequency and percentage. Metrics of central tendency, such mean and standard deviation, were used to assess the Cyber security risk management practices procedures and difficulties.

Open-ended questions were analyzed using qualitative data analysis in respect to the study that was being considered. Furthermore, frequency tables mean, standard deviation, and percentages were used to display the examined data.

Regression analysis used to identify the non – technical factors that significantly influence the effectiveness of cyber security risk management at CBE. By fitting a regression model with the effectiveness of cyber security risk management as the dependent variable and various factors (such as human factors) as independent variables, organizational culture as mediating factor we can determine which factors have the most significant impact on effectiveness. Because this study has more than one predictor variable and want to assess their combined effect on the outcome, this study used multiple linear regression model.

Descriptive analysis techniques used to identify and categorize the challenges faced by CBE during the implementation of cyber security risk management practices. This could involve analyzing qualitative data from interviews, surveys, or documentation to identify recurring themes or patterns related to implementation challenges.

3.6 Validity and Reliability

The creation of the questionnaire was split into several sections in order to increase the validity and reliability of the study. Prior to choosing which items to include in the questionnaire and creating the questionnaire itself, a thorough literature review on cyber security risk management practices, non-technical factors influencing the effectiveness of CSRM, and CSRM challenges was carried out (Face Validity). A pilot study was conducted, too. The stakeholders listed above, who were left out of the final sample of responders, received the questionnaire. They were asked to participate in the investigation after receiving an overview of the study's theoretical foundation. They went over the questions and provided appropriate responses. They also offered their opinions on the questionnaire's overall content validity as well as specific topics.

3.7 Ethical Considerations

The ethical consideration during conducting a research and collecting respective data includes right to choose, right to safety, right to be informed, right to privacy and confidentiality (Akarangaand Makau, 2016). In the study every individual selected to fill the questionnaire will be asked his/her willingness to participate.

To protect a respondent from physical and psychological damaging situations questionnaire will not contain any names referring the respondent. All the respondents will also be informed all aspects of a research task and the use of the data and results, which will be only for academic purpose and for the use in that specific organization. Moreover, ethically, confidentiality concerns will be seriously considered. No names will be included in the questionnaire; codes will be used and no individual respondents will be identified during reporting the findings.

Chapter4
Data analysis, Interpretation and Discussions

In this chapter, the data collected was analyzed and findings were generated. The study contains total sample size of 66. The questionnaires and interview questions were distributed accordingly to 66 staffs of selected cyber security department of CBE. All of them were returned back, which makes response rate 100 percent.

The survey contained four major sections: 1) Demographic Information about the respondents,
2) Assessing the existing cyber security risk management practices 3) Non- technical Factors affecting cyber security risk management practices, with independent variable human factors with 5 sub sections that contain (security awareness and training, behavioral aspect, cognitive load, social influence and psychological factors) and mediator variable Organizational culture and leadership with 3 sub sections (Leadership Commitment, security culture and communication and collaboration)

4) Challenges of implementation cyber security risk management practices With the exception of demographic information and a few inquiries, Likert scaling is used. Scale value 5 indicates Strongly Agree, 4 imply Agree, 3 imply Neutral, 2 indicate Disagree, and 1indicates Strongly Disagree.

4.1Demographic Information about Respondents

To collect demographic Information about the respondents the parameters like Gender, Age, level of Education, Information System cyber security work experience and current position in organization were used.

Table 1demographic Information

Attributes	Description	Frequency	Percent	Valid Percent
Gender	M	49	74.2	74.2
	F	17	25.8	25.8
	20-30	45	68.2	68.2
	30-40	18	27.3	27.3

Age	40-50	1	1.5	1.5
	>50	2	3	3
Level Of Education	Diploma	0	0	0
	Degree	48	72.7	72.7
	Masters	16	24.2	24.2
	PHD	2	3	3
IS security department Experience	<1	13	19.7	19.7
	1-5	41	62.1	62.1
	5-10	10	15.2	15.2
	>10	2	3	3
Current Position in an Organization	Junior Level	32	48.5	3
	Senior Level	32	48.5	48.5
	Managerial Level	2	3	48.5
	Top-level	0	0	0
Total		66	100	100

Source own survey, 2024

Of the 66 respondents who are part of the Cyber security risk management practices, 49 (74.2%) are male and 17 (25.8%) are female. This indicates that most Cyber security department office members are male. In terms of their age, 45 (68.2%) respondents are between 20-30years old, 18(27.3%) between 30-40 years old, only 1 (1.5%) between 40-50years old, and only two (3%) are over 50. This implies most respondents are young adults. Regarding their level of education, there are no Diploma holders among respondents. Instead, 48 (72.7 %) are Degree holders, and16 (24.2) are Master's holders and 2(3%) are PhD holders.

When we look at their departmental experience Work Experience, 13(19.7%) respondents have less than one year of experience, 41 (62.1 %) have one to five years of experience, 10 (38.5%) have five to ten years of experience and only 2 (3%) have more than ten years of experience. The results show that the majority of respondents are seniors.

In terms of their current position, 32 respondents (48.5%) are in low-level positions, 32 (48.5%) are in middle-level positions, 2 (3%) are in managerial positions, and no top-level positions. This indicates that the majority of respondents hold middle-level positions and juniors in an organization.

In general, their demographic information indicates that most of the respondents are seniors having educational qualifications degree and above, and young adults. This added a significant value to the responses gathered.

4.2 Cyber security risk management practices

Assessment of the existing cyber security risk management practices
This subsection of the analysis contains the practices included in the existing CSRM of CBE.

Before analyzing and interpreting data related with assessment of existing CSRM Practices, the validity and reliability of the data were tested using Pearson correlations and Cronbach's alpha.

Table 4.2 assessment of existing cyber security practices questionnaire Reliability test

Reliability Statistics		
Cronbach'sAlpha	Cronbach's Alpha Based on Standardized Items	No of Items
0.820	0.820	8

Table 2 reliability test

Source: ownsurvey2024

Table 3 Descriptive statistics

Attributes	Description	Frequency	Percent	Mean	Standard Deviation
Overall preparedness of managing CSR of CBE is enough	Strongly agree	10	15.2.	3.73	0.775
	agree	31	47.0		
	neutral	*22*	33.3		
	disagree	3	4.5		
	Strongly disagree	0	0		
Commercial Bank's incident response procedures are effective in addressing cyber security incidents	Strongly agree	9	13.6	3.74	0.771
	agree	35	53		
	neutral	18	27.3		
	disagree	4	6.1		

	Strongly disagree	0	0		
CBE has implemented best security controls (e.g., firewalls, antivirus software) to protect against cyber threats	Strongly agree	27	40.9	4.17	0.796
	Agree	23	34.8		
	Neutral	16	24.2		
	Disagree	0	0		
	Strongly disagree	0	0		
CBE provides adequate cyber security training and awareness programs to its employees	Strongly agree	10	15.2	3.58	0.929
	Agree	28	42.4		
	Neutral	18	27.3		
	Disagree	10	15.2		
	Strongly disagree	0	0		
CBE is highly compliant with relevant cyber security regulations and industry standards	Strongly agree	4	6.1	3.77	0.549
	Agree	43	65.1		
	Neutral	19	28.8		
	Disagree	0	0		
	Strongly disagree	0	0		
The communication and reporting mechanisms in place for cyber security incidents within CBE is satisfactory	Strongly agree	3	4.5	3.50	0.856
	Agree	39	59.1		
	Neutral	12	18.2		
	Disagree	12	18.2		
	Strongly disagree	0	0		
CBE invests sufficient resources in cyber security measures to adequately protect against cyber threats	Strongly agree	12	18.2	3.97	0.656
	Agree	41	62.1		
	Neutral	12	18.2		
	Disagree	1	1.5		
	Strongly disagree	0	0		
	Strongly	15	24.3		

CBE is proactive in continuously improving its cyber security practices in response to evolving threats and vulnerabilities	agree			3.92	0.771
	Agree	33	50		
	Neutral	16	22.7		
	Disagree	2	3		
	Strongly disagree	0	0		

Source: ownsurvey2024

Descriptive statistics of the variables

The table below shows the descriptive statistics of the assessment of existing Cyber security risk management practices of commercial bank of Ethiopia. The results in the table show that CBE has implemented best security controls (e.g., firewalls, antivirus software) to protect against cyber threats had the highest mean score of 4.17, followed by CBE invests sufficient resources in cyber security measures to adequately protect against cyber threats with an overall mean score of 3.97,and The communication and reporting mechanisms in place for cyber security incidents within CBE is satisfactory with a relatively low overall mean score of 3.50 and another relative low CBE provides adequate cyber security training and awareness programs to its employees with mean score of 3.58. These shows, from the employee point of view commercial banks in Ethiopia, implemented best cyber security controls regarding tools and investing sufficient resources but it has poor communication and reporting mechanism following inadequate cyber security awareness and training programs.

Non-technical factors affecting effectiveness of cyber security risk management practices

4.2.2.1 Rating of variables

Reliability test

The calculation of reliability is done so that it shows the reliability of the average of the things rather than the reliability of any particular item. For instance, all of the latent variables and the indicator variables that matched them were multi-item questions, as can be seen in the factor loading table below. A single item question yields less reliable results than a summarized multi-item question (Gliem & Gliem, 2003). The five indicator factors that made up the human element—an exogenous variable in this study—were behavioral aspect, psychological component, social influence, cognitive load, and security awareness and training. The study uses

communication and collaboration, corporate culture, and leadership commitment as mediator factors. According to the study, the sum of the variables has an average Cronbach's alpha value of 0.891, and the study's reliability test is in the "excellent" range.

Table 4 reliability test of variables using cronbach alpha value

	Reliability Statistics				
No	Variable Name	Cronbach's Alpha Value	Cronbach's Alpha Based on standardized items	No of items	(α) reliability ranges
Independent variables					
1	Security awareness and training	0.816	0.816	3	Good
2	Behavioral aspect	0.706	0.706	3	Acceptable
3	Psychological factor	0.712	0.712	3	Acceptable
4	Cognitive load	0.774	0.774	3	Acceptable
5	Social influence	0.706	0.703	3	Acceptable
Mediator variables					
1	Leadership commitment	0.755	0.755	3	Acceptable
2	Security culture	0.706	0.706	3	Acceptable
3	Communication collaboration				
Dependent variable					
1	Effectiveness of cyber security practices	0.776	0.776	4	Acceptable
	Overall	0.891	0.891	28	Excellent

Source: Own computation using SPSS of the survey, 2024

Three main variables were used in this study: the independent variables were security awareness and training, behavioral aspect, psychological aspect, cognitive load, and social influence; the dependent variable was the effectiveness of cyber security risk management practices; and the mediator was organizational culture and leadership. Using descriptive statistics, the central tendency (SD, mean, and mode) was used to rate these variables. The following summarizes the outcome: respondent dependent variables, mediator variables, and independent variables. The behavioral, psychological, cognitive load, social influence, security awareness, and training aspects of human-related elements (independent variables) were examined in this study. Organizational factor and leadership as a mediation factor which includes leadership commitment, security culture and communication and collaboration and effectiveness of cyber security risk management practices as dependent variable. In this study, all variables were

assessed with three items where respondents 'over all mean rating of each items that consists effectiveness which is assessed by four items in the questionnaire were measured using five-point Likert scale

4.2.1 Correlation analysis

Correlation analysis of the variables is presented below

Table 4 correlation statistics independent with dependent variables

Correlations

		Security awareness and training	Behavioral aspect	Psychological factor	Cognitive load	Social influence	Effectiv CSRM
Security awareness and training	Pearson Correlation	1	.438**	.456**	.354**	.564**	.077
	Sig. (2-tailed)		.000	.000	.004	.000	.043
	N	66	66	66	66	66	66
Behavioral aspect	Pearson Correlation	.438**	1	.654**	.238	.355**	.105
	Sig. (2-tailed)	.000		.000	.055	.003	.034
	N	66	66	66	66	66	66
Psychological factor	Pearson Correlation	.456**	.654**	1	.265*	.646**	-.041
	Sig. (2-tailed)	.000	.000		.032	.000	.743
	N	66	66	66	66	66	66
Cognitive load	Pearson Correlation	.354**	.238	.265*	1	.568**	.020

	Sig. (2-tailed)	.004	.055	.032		.000	.025
	N	66	66	66	66	66	66
Social influence	Pearson Correlation	.564**	.355**	.646**	.568**	1	.040
	Sig. (2-tailed)	.000	.003	.000	.000		.052
	N	66	66	66	66	66	66
Effectiveness of CSRM	Pearson Correlation	0.77	.205	-.041	-.020	.040	1
	Sig. (2-tailed)	.043	.034	.0743	.025	.052	
	N	66	66	66	66	66	66

Source: Own computation using SPSS of the survey, 2024

As per the correlation table, 4.5 above, effectiveness of CSRM has a positive relationship with Security awareness and training, Behavioral aspect, Cognitive load and Social influence. The correlations clearly show that effectiveness of CSRM strongly positive and statistically significant relationship with the aforementioned explanatory variable.

4.2.2 Regression Analysis

Regression analysis is a statistical technique that is used to estimate the relationships between endogenous and exogenous variables. It allows for the determination of the strength of the relationship between variables as well as the predictive power of the independent variables on the dependent variable. In short, regression helps a researcher understand how much a changeinthevalueofthedependentvariablecausesachangeinthevalueoftheindependentvariableswhile the other independent variables remain constant. Regression analysis is a statistical method for

determining which variables affect. While there are many different types of regression analysis, they all focus on the impact of one or more independent variables on a dependent variable.

Aspect	Mode	Mean	Standard Deviation
Organizational culture and leadership			
Leadership commitment	3	3.5	0.66
Security culture	3	3.26	0.74
Communication and collaboration	4	3.5	0.76
Human factors			
Security awareness and training	4	3.72	0.74
Behavioral aspect	5	4.27	0.628
Psychological factor	4	4.13	0.60
Cognitive load	4	3.73	0.66
Social influence	4	3.89	0.558
Effectiveness of CSRM	4	3.7	0.34

Table 5 regression analysis

Source: survey. 2024

Diagnostic Tests of Assumptions of Classical Linear Regression Model (CLRM)

Homoscedasticity Test

One of the assumptions of ordinary least squares estimation of homoscedasticity tests, if the errors in linear regression model have a common variance or equally distributed. If residuals have constant variance, it is said homoscedastic. In a linear regression the data is homoscedastic if it looks somewhat like short-gun blast of randomly distributed data. Accordingly, the data was tested and fund that residuals are equally distributed. This is shown below in figure 4.4. It describes a situation in which the error term (random disturbance in the relationship between the

independent variables and the dependent variables) is the same for all independent variable values.Ascatterplotdiagramlistedbelowusedtotestassumptions.Theoutputplotsthevaluespredicted by the model against the residuals obtained. The variation in the residuals should beroughlysimilarasthepredictedvaluesincrease.Thegraphappearstobearandomarrayof dots. As a result, the model is homoscedasticity.

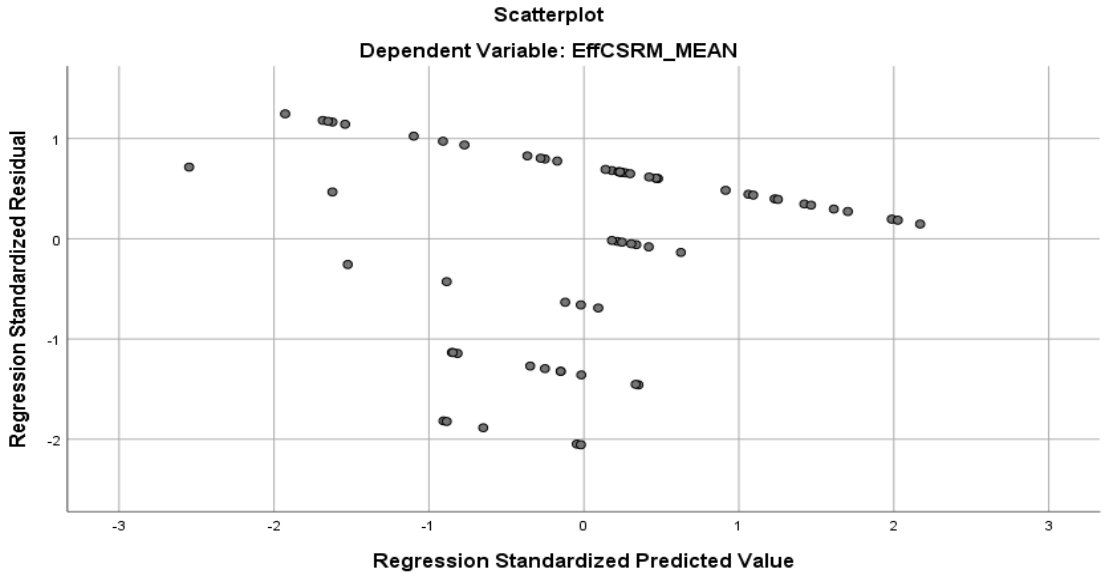


Figure 2 p-p plot

Source: Own survey data (2024)

Test on normality of residuals

A normality test is used to determine whether the error term is zero mean and constant variance in the model. Normality test is one of the additional assumptions of linear classical ordinary least Square method. Multiple regressions necessitate that the residuals be normally distributed. Skewness and kurtosis are statistical tools that can be used to determine whether or not data is normally distributed. Different test methods were conducted to test normality in the given regression model from these kurtosis and skewness distribution, normal probability plot, and Histogram plot test. In this study Histogram plot test is performed to check the test. The graph below indicated that the error term distribution in the model is normally distributed.

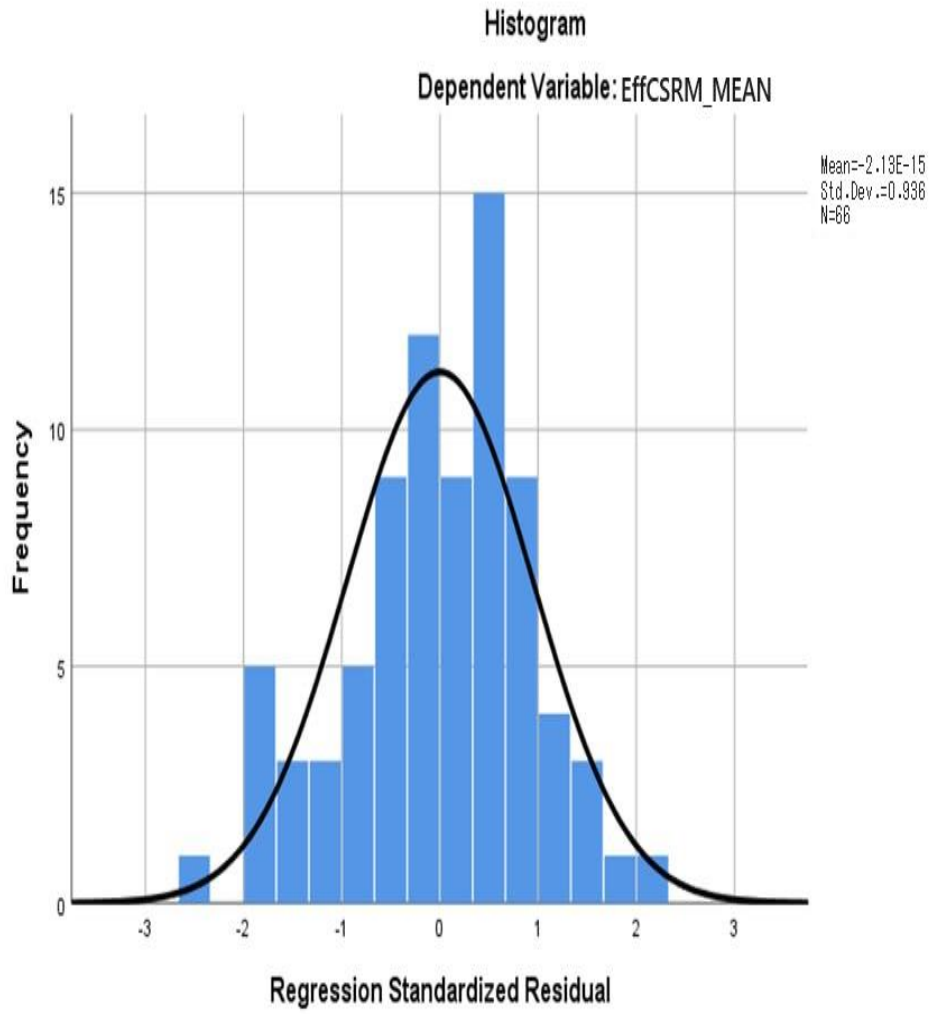


Figure 3 Histogram

Autocorrelation Test

The Durbin-Watson statistic is used to determine whether or not there is a serial correlation among the residuals. If the Durbin-Watson statistic is close to2 and the acceptable range is 1.50-2.50, the residuals are not correlated. As shown in the table, the Durbin-Watson statistic value is 1.702, which is close to greater than 1.5, indicating that there is no autocorrelation problem in this model.

According to Will Kenton (2019), Durbin Watson (DW) statistic is a test for autocorrelation in the residuals from a statistical regression analysis. According to Kenton, the Durbin-Watson statistic will always have a value between 0 and 4. A value of 2.0 means there is no

autocorrelation detected in the sample. Values from0 to less than 2 indicate positive auto correlation and values from2 to 4indicate negative autocorrelation.

In order to test whether autocorrelation of residuals from the linear regression models are existing or not in this study, Durbin-Watson test statistic was used. The Durbin-Watson test statistic ranges from a value close to zero, which denotes positive autocorrelation, to a value near to four which suggests negative autocorrelation. The commonly used benchmark is that values of Durbin-Watson (d) which fall in the range between1.5 to 2.5 indicates non-existence of residual autocorrelation. As it is shown in Table 4.5, the calculated Durbin-Watson test statistic (d=1.702) is within the range of 1.5 and 2.5indicatingthat there is no autocorrelation among the variables.

The computed Durbin-Watson test statistics showninTable4.7

Model

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R square change	Durbin-Watson
1	.460a	0.47	0.32	0. 354	0.47	
2	.475b	0.76	0.54	0.354	0.29	1.702

Summary

Table 6 model summary

Predictors :(Constant), independent variables ;(SAT, BA, CL, PSYF and SI) adding mediating variables (LC, SC and CC)

Dependent variable: Effectiveness of CSRM

Table 4.7Testingfor autocorrelation

Source: Own survey data (2024)

Multi-co linearity

According to Myers (1990) Multi-co linearity refers to _very high inter-correlation among predicator variables.

A perfect linear relationship among the independent variables implies difficulty of computing unique estimates for a regression model. As the degree of multi-co linearity increases, the estimates from the regression model become unstable and hence it would be difficult to discrete the separate effect of predictor variables.

If the model contains a correlation or r/s b/n explanatory variables, multicollinearity will occur. It is difficult to separate the effect of each independent variable from the dependent variable in the case of multicollinearity in the regression model (Brooks, 2008). In various kinds of literature, various tests were used to determine the presence of a high multicollinearity problem in a given model. In the literature, the correlation matrix and the variance inflation factor (VIF) were commonly used. According to Sekaran and Bougie (2016), the acceptable tolerance and variance inflation factor (VIF) values are greater than 0.10 and less than 10. According to table 4.7, each tolerance and VIF value of the independent variable and the mediating variable is greater than 0.1 and less than 10

Therefore, the model in this thesis has no multicollinearity problem.

In addition, the standard errors for the coefficients would be highly inflated. Variance inflation factor (VIF) was used to check the seriousness of multi-co linearity among explanatory variables. As a rule of thumb, multi-co linearity is a potential problem when VIF is greater than 4; and, a serious problem when it is greater than 10. According to Myers (1990) a variable having VIF greater than ten indicates high multi-co linearity which requires further investigation. VIFs were calculated for all predicator variables except combination were found to be less than ten and the tolerance level is less than two implying that multi-co linearity was not a concern in this study. Hence, if a bivariate correlation between predictor variables is less than 0.8, it shows multi-co linearity is not a serious concern.

Constructs	Co linearity statistic		sign
	Tolerance	VIF	
Security awareness and training (SAT)	.533	1.875	.926
Behavioral aspect (BA)	.468	2.137	.309
Psychological factor(PSYF)	.349	2.867	.184
Cognitive load (CL)	.429	2.331	.849
Social influence (SI)	.342	2.923	.416
	.		.
Leadership commitment (LC)	.292	1.298	.770

Security culture (SC)	.624	1.973	.507
Communication and collaboration(CC)	.492	2.763	.362

Table 7 co linearity

Dependent Variable: Effectiveness of CSRM

Source: own survey 2024

Table 4.7 Multi-Co linearity Tests

Linearity test

A linearity test is often conducted as part of statistical analysis, especially in regression analysis. This test assesses whether the relationship between two variables is linear. The graph below typically includes a scatter plot of the data points with a fitted line visually inspecting this graph to assess the linearity of the relationship. The data points form a roughly straight line; the relationship is likely linear. This means that the relationship between the independent and dependent variables can be adequately modeled using linear regression techniques.

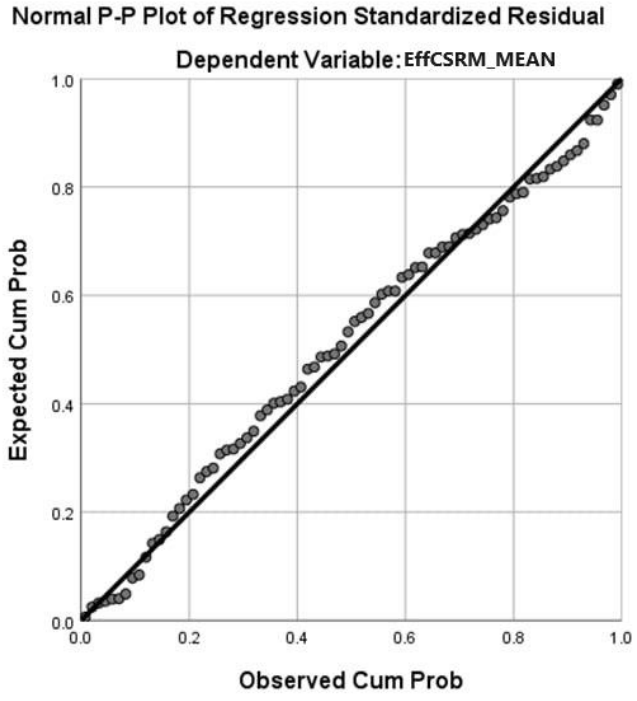


Table 8 linearity test

4.2.3 Regression and Mediation analysis

This analysis is performed to test the first hand effect of independent variable on mediating variables (assuming mediating variables as dependent) before testing indirect effect of the independent variables on the dependent variable

Table 9 Model one (leadership commitment as dependent variable)

P value need to be <0.05

Variables	Coefficient	Std.Err.	t-statistic	p-value
Security A &T	0.000	0.131	0.001	0.009
Behavioral A	0.162	0.166	-0.999	0.022
Psychological F	0.172	0.212	0.890	0.377
Cognitive Load	0.316	0.143	2.187	0.033
Social influence	0.124	0.233	0.634	0.028
	-			

Table 10: Model two (Security culture as dependent variable)

Variables	Coefficient	Std.Err.	t-statistic	p-value
Security A &T	0.286	0.136	2.106	0.039
Behavioral A	-0.155	0.171	-1.037	0.304
Psychological F	0.040	0.219	0.221	0.826
Cognitive Load	0.494	0.148	3.700	0.000
Social influence	-0.082	0.240	-0.452	0.043
	.			.

Table 11 Model three (communication and collaboration as dependent variable)

Variables	Coefficient	Std.Err.	t-statistic	p-value
Security A &T	0.325	0.117	2.858	0.006
Behavioral A	0.119	0.148	0.951	0.345
Psychological F	0.049	0.189	0.329	0.044
Cognitive Load	0.431	0.127	3.855	0.000
Social influence	0.022	0.207	0.144	0.050

Table 12Model four (effectiveness of CSRM as dependent variable)

Variables	Coefficient	Std.Err.	t-statistic	p-value
Security A &T	0.439	0.082	0.094	0.010
Behavioral A	0.247	0.100	1.027	0.038
Psychological F	-0.312	0.125	-1.344	0.145
Cognitive Load	-0.066	0.101	-.0191	0.048
Social influence	-0.170	0.136	0.819	0.206
Leadership commitment	0.154	0.077	-1.064	0.032
Security culture (	0.088	0.084	-0.492	0.024
Communication collaboration(CC	0.146	0.097	0.692	0.043

4.2.3.1 Regression output and results

As per regression output above in model three: from the total of five independent variables three variables. Security awareness and training, cognitive load and behavioral aspect are significant effect on the effectiveness of CSRM practices of Commercial Bank of Ethiopia. But the remaining two variables, i.e. psychological factor and social influence were insignificant effects on effectiveness of CSRM practices of CBE.

Security awareness and training

According to the results of the regression, the coefficient of security awareness and training has a positive and statistically significant effect on effectiveness of CSRM practices. This means that if security awareness and training program improves by one unit, effectiveness of CSRM increases by 0.439, assuming all other variables remain constant.

Behavioral aspect

According to the model's regression output, the coefficient of gender diversity is positive and

statistically significant at the 6.8% level of significance. If all other variables remain constant, one-unit increase in behavioral aspect leads to a 0.247-unit increase effectiveness of CSRM practices.

Cognitive load

In the regression output, the coefficient of cognitive load is a negative and statistically significant effect on effectiveness of CSRM in CBE at a 7.5 % level of significance. This implies that when cognitive load increased by one unit then the level of effectiveness of CSRM practices decreased by 0.06 units being other explanatory variables constant.

Social influence and psychological factors

Both affect the effectiveness negatively and insignificant compared to the other independent variables

Mediation is a hypothesized causal chain in which one variable affects a second variable that, in turn, affects a third variable. The intervening variable, M, is the mediator. It "mediates" the relationship between a predictor, X, and an outcome.

Once the model was tested for its fitness with observed data, the contribution of the mediating variable (leadership commitment, security culture and communication and collaboration) performed using SPSS. First, independent variable (x) should influence effectiveness second; independent variable (x) should influence the mediating variable (M).Third, the mediating variable (M) should influence effectiveness of CSRM(y).

Generally, test the impact of mediator variable through three regression model. Theseregressionmodelsarearegressionmodelbetweendependentindependentvariables, a regression model between mediator variables independent variables, and a regression model between a dependent variable and both independent variable and mediator variable. If the mediator variable significantly affects the dependent variable there is mediation effect in the model.

Model one

As per model one presents the relation between the mediator variable of leadership commitment and independent variables. The regression output implies that dependent variables (security awareness and training, behavioral aspect, social influence) has appositive and significant effect on leadership commitment. But, psychological factor is an insignificant effect on leadership commitment.

Model two

Model two presents the relationship between the mediator variable of security culture and independent variables. The regression output implies that out of five variables security awareness and training and cognitive load positively and significantly affect security culture of CBE but psychological factor and behavioral aspects are insignificant while social influence is significant but negatively affects security culture of CBE

Model three

Model three presents the relationship between the mediator variable of communication and collaboration and independent variables. The regression output implies that except behavioral aspect all the remaining variables affect significantly and positively the communication and collaboration activity of CBE

Model four

Model four presents the regression output of the dependent variable with independent and mediator variables. In this mode, the effect of mediator variables i.e. leadership commitment, security culture and communication and collaboration of commercial bank of Ethiopia is positive and statistically significant affects effectiveness of CSRM practices. The coefficient of the mediator variables implies that a one-unit increase in leadership commitment, security culture and communication and collaboration leads to 0.15,0.08 and 0.14-unit increase in effectiveness of CSRM practices respectively. Concerning the mediating role of leadership commitment, security culture and communication and collaboration in the relationship between human factors and effectiveness of CSRM practices in CBE; organizational culture and leadership there is a mediating role in the relationship between dependent and independent variables since there is a significant effect of mediator variable on the dependent variable and independent variable on the mediatory variable. In this study the mediator variable mediates in the relationship between effectiveness and human factors is partial since there is a significant relationship between dependent and independent variables.

4.2.4 Challenges of implementing cyber security practices

This subsection of the analysis contains the practices includes the challenges for implementation of CSRM practices within CBE. Cronbach's alpha was used to test the reliability of the collected data.

Table 13*challenges of implementations questionnaire Reliability test*

Reliability Statistics		
Cronbach'sAlpha	ıbach's Alpha Based on Standardized Items	No of Items
0.7	0.7	5

Source: own survey2024

As shown in the table above the cronbach's Alpha was 0.7, which is an acceptable value. Thecronbach'sAlphavaluegreaterthan0.7isconsideredtobe acceptable; therefore, the questionnaires used to collect challenges of CSRM practices were reliable.

Table 14*challenges of implanting cyber security risk management Practice*

Attributes	Description	Frequency	Percent	Mean	Standard Deviation
There is high extent of resource constraints (e.g., budget, staffing) as a hindrance to effective implementation of cyber security measures at CBE	Strongly agree	7	10.6	3.18	0.493
	Agree	12	18.2		
	Neutral	33	50.0		
	Disagree	14	21.2		
	Strongly disagree	0	0		
There are high challenging of technological complexities of implementing cyber security solutions within CBE	Strongly agree	0	0	2.61	0.562
	Agree	9	13.6		
	Neutral	24	36.4		
	Disagree	31	47.0		
	Strongly disagree	2	3		

There is a high extent of employee resistance to change poses a barrier to the successful implementation of cyber security initiatives at CBE	Strongly agree	2	3	3.12	0.414
	Agree	20	30.3		
	Neutral	28	42.4		
	Disagree	16	24.2		
	Strongly disagree	0	0		
There are high extent of the burden of regulatory compliance impede the implementation of cyber security measures at CBE	Strongly agree	2	3	3.17	0.446
	Agree	14	21.2		
	Neutral	43	65.2		
	Disagree	7	10.6		
	Strongly disagree	0	0		
There are high concerns about the risks associated with third-party vendors or suppliers who have access to Commercial Bank's systems or data	Strongly agree	8	12.1	3.41	0.528
	Agree	23	34.8		
	Neutral	23	34.8		
	Disagree	12	18.2		
	Strongly disagree	0	0		

Source: own survey 2024

To assess the challenges of implementing cyber security risk management practices, the respondents were asked 5 questions based on likert scale. Which is calculated based on the response results, indicated that high concerns about the risks associated with third-party vendors or suppliers who have access to Commercial Bank's systems or data are among the first ranked challenges with mean of 3.41, and standard deviation of 0. 928. None of the respondents strongly disagreed or disagreed with the issue. In contrast, 8 (14.1%) strongly agreed and the remaining 23 (34.8%) agreed with the issue.

According to the respondents, the second-ranked challenge that the firm usually faces was There is high extent of resource constraints (e.g., budget, staffing) as a hindrance to effective implementation of cyber security measures at CBE and its mean and standard deviation were 3.18 and 0.893 respectively. None of the respondents strongly disagreed and only 14 (21.2%) disagreed with the issue. 12 (18.2%) agreed, 7 (10.6%) strongly agreed, and 33(50%) were neutral. This result implies that resource constraint is also the most common challenge in the firm following the challenge of gathering and analyzing all the necessary data.

Finally, the challenges ranked fourth and fifth, according to the respondents' response, there is a high extent of employee resistance to change poses a barrier to the successful implementation of cyber security initiatives at CBE 16 disagreed (24.2) and there is high challenging of technological complexities of implementing cyber security solutions within CBE 2(3%) strongly disagree and 31(40%) disagreed. this shows that the technology complexity is not considered as a challenge and there is no also significant employee resistance to change for the successful implementation of cyber security risk management practices.

Major Findings and Relation to Previous Studies

Third-Party Vendor Risks:

Relation to Prior Research: Prior studies (e.g., Herath & Rao, 2009; Vance et al., 2012) have continuously emphasized the importance of third-party vendor risks in cyber security and the necessity of implementing strong third-party risk management (TPRM) procedures.

New Contribution: With particular data from CBE, your study validates these worries and demonstrates that respondents generally agree on the seriousness of third-party risks. It provides context-specific insights on the ways in which these risks appear in Ethiopia's banking industry

Resource Constraints:

Relation to Previous Studies: Research has acknowledged resource constraints, including budget limitations and staffing shortages, as common challenges in cyber security risk management (e.g., Lai & Li, 2005; Hu et al., 2012).

New Contribution: Using Likert scale replies as empirical evidence, your study quantifies these CBE problems. It highlights how resource limitations are a global issue while providing particular information pertinent to Ethiopia's banking sector.

Employee Opposition to Change:

Relation to Previous Research: Organizational change literature has highlighted employee resistance to change and its effect on cyber security activities (e.g., Meske & Stieglitz, 2013).

New Contribution: While identified as a challenge, your study indicates that employee resistance to change may not be as pronounced compared to other challenges like third-party risks and

resource constraints. This nuanced understanding contributes to targeted strategies in managing organizational change for cyber security improvements.

Technological Complexities:

Relevance to Previous Research: Research has frequently shown that technological complexity is a barrier to the implementation of cyber security effectively (e.g., Straub et al., 2004).

New Contribution: Contrary to predictions, the majority of respondents at CBE do not view technological complexity as a significant challenge, according to your study. This conclusion casts doubt on presumptions and points to a higher level of readiness or trust in the organization's ability to handle the technological components of cyber security.

What is New about This Study?

Contextual Specificity: This study provides specific insights into cyber security challenges faced by the Commercial Bank of Ethiopia, offering a localized perspective that may differ from global or generalized findings.

Quantitative Assessment: By using Likert scale responses; this study quantifies perceptions and concerns, providing a structured analysis of cyber security challenges within CBE.

Practical Recommendations: The study suggests practical mitigation strategies tailored to address identified challenges, such as enhancing TPRM practices and optimizing resource allocation despite constraints.

By using Likert scale replies as empirical evidence; this study quantifies these CBE problems. It highlights how resource limitations are a global issue while providing particular information pertinent to Ethiopia's banking sector. Employee Opposition to Change: Connection to Other Research: The research on organizational change has highlighted employee resistance to change and how it affects cyber security activities (e.g., Meske & Stieglitz, 2013). Fresh Input: Employee resistance to change has been cited as a challenge, but your research suggests that it may not be as significant as other challenges like resource limits and third-party risks. This detailed understanding supports focused organizational change management tactics for advancements in cyber security. Technological Complexities: Connection to Past Research:

Research has frequently indicated that technological complexity is a hindrance to the successful deployment of cyber security (Straub et al., 2004)).

New Contribution: This research reveals that, in contrast to predictions, the majority of respondents at CBE do not view technical complexity as a significant obstacle. This conclusion casts doubt on presumptions and points to a higher level of readiness or trust in the organization's ability to handle the technological components of cyber security. What Makes This Study New? Contextual Specificity: This study offers a localized perspective that may vary from global or generalized findings, providing specific insights into cyber security concerns encountered by the Commercial Bank of Ethiopia.

Quantitative Assessment: This study provides a structured investigation of cyber security challenges inside CBE by quantifying views and concerns through the use of Likert scale responses.

Practical Suggestions: This study makes recommendations for realistic mitigation techniques that are suited to deal with the issues found, like improving TPRM procedures and optimizing resource allocation despite constraints.

Chapter5
Summary, Conclusion and Recommendation

Introduction

The study's summary of findings, conclusion, and recommendation are presented in this chapter. The goal of the study was to determine the current CSRM practices, the impact of non-technical elements on the efficacy of CSRM practices, and the difficulties associated with implementing CSRM practices in Ethiopia's commercial banks.Additionally, it attempted to offer fresh empirical data on the leadership and organisational culture's mediating roles in the relationship between human factors and the efficacy of Commercial Bank of Ethiopia's cyber security risk management procedures.

5.1 Summary

A self-administered survey was used to gather 66 (100%) of the questionnaires, and 66 (100%) of the questionnaires were filled out correctly and prepared for analysis. Statistical programme for social science software (SPSS) was used to reanalyse the data that had been gathered. To test the hypotheses, regression analysis and mediation analysis were used. In addition to various post-estimation tests like multicollinearity, normalcy, and homoscedasticity tests, regression analysis, reliability, and correlation analysis were carried out.

The purpose of the reliability test was to determine the validity and reliability of the questionnaire. With an overall Cronbach's Alpha result of 0.82, 0.89, and 0.7 for each of the three objectives, the questionnaire was deemed satisfactory and dependable. Table 4.1 shows the demographics of the respondents. Of the 66 respondents who are involved in the cyber security risk management processes, 49 (74.2%) are male workers. This suggests that men predominate in the cyber security department's office staff. 45 (68.2%) of the respondents are between the ages of 20 and 30, indicating that young adults make up the majority of the sample. In terms of education, the majority of 48 (72.7%) have a degree. The bulk of responders are seniors, as seen by the departmental experience Work Experience 41 (62.1%), which has one to five years of experience.

Regarding their present roles, 32 respondents (48.5%) hold low-level posts, while 32 respondents (48.5%) hold middle-level positions. This suggests that most respondents are junior position in an organisation and have middle-level positions.

According to their demographic data, the majority of respondents are young adults and seniors with degrees or higher in education. This gave the responses received a considerable boost in value.

The assessment of the CBE's current CSRM processes analysed using descriptive analysis to demonstrate that descriptive statistics of the evaluation of the commercial bank of Ethiopia's current cyber security risk management procedures are displayed in table 4.3 above. The table's results demonstrate that CBE has the highest mean score (μ4.17) for using the finest security controls (firewalls, antivirus software, etc.) to protect against cyber threats. With a relatively low total score of μ 3.50, the CBE's cyber security incident reporting and communication methods are deemed inadequate. From the perspective of the employees, these shows

From the perspective of the employees, they demonstrate that although commercial banks in Ethiopia have adequate resources and have adopted the strongest cyber security measures in terms of technologies, their reporting and communication systems are deficient.

The impact of human factors on the efficiency of CSRM in the commercial bank banking sector Ethiopia: leadership and organisational culture as mediating factors. Five independent human factors variables—security awareness training, behavioural aspect, psychological factor, cognitive load, and social influence—as well as two mediating variables—leadership commitment, security culture, and communication and collaboration—were identified based on the literature review covered in chapter two.

Multiple regression analysis was used to investigate how the human factor affected the effectiveness of CSRM in the banking sector of Commercial Bank Ethiopia. Three of the five independent factors had a substantial impact on effectiveness of CSRM practices Commercial bank of Ethiopia, according to the analysis's findings. These include behavioural aspects, cognitive load, and security awareness and training. However, social effects and psychological factors had a negligible impact on effectiveness.

The mediation analysis further verified that a portion of the relationship between the effectiveness of CSRM and human factors in CBE is mediated by leadership commitment, security culture, communication, and collaboration.

.

The company faces two main challenges when implementing cyber security risk management practices: (1) a high degree of resource constraints and (2) third-party vendors or suppliers who have access to Commercial Bank's systems or data ($\mu = 3.41$). The high level of employee resistance to change ($\mu = 3.12$) comes next.

5.2 Conclusions

The study's main objectives are as follows: first, it assesses current cyber security management practices based on employee feedback. Commercial banks of Ethiopia have the best cyber security controls in terms of tools and resources invested, but reporting and communication systems are poor and its cyber security awareness and training programmes are inadequate.
The mediating function of organisational security culture and leadership is another goal that aims to affect non-technical elements in the efficacy of CBE's cyber security risk management methods. The study came to the following conclusions based on its findings:

The study's findings demonstrated the favourable and significant effects of security awareness and training on the efficiency of CSRM procedures. It implies that continuous security awareness training and personnel training will boost the effectiveness of CSRM.
The study's conclusions verified that behavioural factors had a favourable and substantial impact on CSRM effectiveness. This suggests that the degree to which CSRM in CBE is successful rises in parallel with the behavioural aspect of employee awareness of cyber security.
The study findings validated that there is a significant and adverse impact of cognitive load on the effectiveness of CSRM. This suggests that when workers' cognitive burden in the cyber security workplace rises, the degree of effectiveness of CSRM in CBE decreases.

The study's findings demonstrated that leadership commitment acts as a partial mediator between human factors and the effectiveness of CSRM. This suggests that the human element has an impact on efficacy both directly and indirectly through leadership commitment.
The study's findings demonstrated that security culture mediates, to some extent, the impact of human variables on the efficacy of CSRM techniques. This suggests that the human factor has a dual impact on effectiveness: directly and through security culture.
As a mediator variable, cooperation and communication are equivalent.
The study finding shows that the company challenges for the implementation of cyber security risk management practices are a high degree of resource constraints and third-party vendors or suppliers who have access to Commercial Bank's systems.
The company faces two main challenges when implementing cyber security risk management practices: a high degree of resource constraints and third-party vendors or suppliers who have access to Commercial Bank's systems or data.

5.3 Recommendation

The conclusion drawn from the research's key findings informs the recommendations that follow. They are listed in the following order: The bank should continue to uphold its reputation for using the best security control technologies and allocating enough funds to defend against cyber threats. But, the bank should regularly update its cyber security reporting and communication systems, as well as security awareness and training initiatives, as human capital is the primary resource in which it should consider investing based on the feedback it receives.

There is a noteworthy correlation between the human factor variables of security awareness and training efficacy under investigation. Ethiopian commercial banks should therefore know how to close the knowledge gap among their staff by investing in cyber security awareness and training. They should also teach staff members about potential threats, safe practices, and the value of upholding protocols to minimise human error. Finally, by fostering a proactive defence culture and offering ongoing, engaging, and pertinent training, CBE can enable staff members to serve as the first line of defence against cyber threats.

Human behaviour frequently determines how well security policies and practices are implemented and followed, as there is a significant positive relationship between the behavioural aspect variable and cognitive load and effectiveness. As a result, the effectiveness of cyber security risk management practices depends on both technical and behavioural components.

Employees must therefore have a high degree of awareness in order to recognise and report dangers proactively and to consistently follow security procedures. It is imperative that employees enhance their awareness of the possible consequences of security breaches. This can lead to a reduction in irresponsibility and an increase in dedication, both of which can boost effectiveness.

Understanding cognitive load is essential for developing efficient security procedures that do not overwhelm users in the context of cyber security risk management, guaranteeing they can adhere to protocols without excessive mental strain so CBE needs to simplify security tasks (clear instructions user friendly interfaces), interactive trainings, automation of routine tasks and positive reinforcement mechanisms.

Leadership commitment, security culture and communication and collaboration have a mediator role in the relationship between effectiveness of CSRM practices and human factors in CBE. Therefore, the bank should focus, maintain and improve the level of leadership commitment, security culture and communication and collaboration through the above human factors in order to get a better result

The responses collected from interview questions and open-ended questionnaires indicated that activities such as third party vendors risk, financial constraints and dynamic changes of digital environments are the challenges which could limit successful implementation. Interview respondents also revealed that data security privacy risks, cyber security risks, quality control risks and intellectual property risks may happen to mitigate this challenges the bank should implement TPRM (third party risk management) strategies like due diligence, clear contract and SLA (service level agreements) vendor audits and so on.

On the other hand, financial constraints are also challenges causing budget limitations, staff shortage due to budget, training and development constraints, incident response limitation because of limited resource can hinder ability to detect and respond security incidents so in order

to mitigate this issues the banks need to prioritize most critical assets, investing in automation tools, internal training programs.

5.4 Suggestion for future research

The scope of this study was restricted to the head office level cyber security department of commercial banks in Ethiopia. As a result, more research on other sectors, like operational level employees, should be done. Because non-technical factors or human factors have distinct dimensions, the study also recommends that additional research be done on the relationship between non-technical factors and the efficacy of CSRM techniques in other industries by integrating more non-technical factor dimension variables.

In order to fully comprehend the study's issue and its excellent research findings, the researcher further recommends that this study be repeated at other comparable financial organisations. This is a result of the study's limitation to one company, Ethiopia's Commercial Bank.

References

Akaranga, S., I. and Makau. L., K. (2016). Ethical Considerations and their Applications to Research's Case of the University of Nairobi. Journal of Educational Policy and Entrepreneurial Research ISSN: 2408-770X (Print), ISSN: 2408-6231 (Online) Vol. 3, N0.12. Pp 1-9, Available at https://profiles.uonbi.ac.ke/kuria_paul/files/429-825-2-pb.pdf

Bahari, S. F. (2010). Qualitative versus quantitative research strategies: Contrasting epistemological and ontological assumptions. Journal Technologies, 52, 17–28

Brown, R., et al. (2021). "Cyber Security Awareness and Training Programs: A Case Study Analysis of Banking Institutions." *Journal of Cyber Security Research*, 10(1), 45-60.

Brown, R., Johnson, S., & Martinez, E. (2021). "Cyber Security Incident Response Planning in Banking: Best Practices." *Journal of Banking and Finance Security*, 14(2), 45-58.

Choi, Y., Kim, J., & Kim, S. (2019). Cyber security risk management practices in banking sector: focusing on the application of ISMS. *Symmetry*, 11(11), 1407.

Collis, J., & Hussey, R. (2009). Business research: A practical guide for undergraduate and postgraduate students (3rd ed.). Basingstoke: Palgrave Macmillan

Cyber Risk Management in Banks: Cyber Risk Bankalarda Siber :Risklerin Yönetimi: Siber Risk Sigortası, November 2018

Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia: Towards Tailoring Cyber Security Framework, Tewodros Getaneh, June- 2018

Cyber security Risk Assessment and Management in Banking. Smith, J. (2020)

Davis, C., Smith, R., & Johnson, T. (2020). "Cyber Threat Intelligence Sharing in the Banking Sector: Strategies and Benefits." *Journal of Financial Cyber security*, 13(1), 78-91.

Finance and Cyber Security Risk Management, Dominguez, Virgilio. (2018).

Garcia, M., & Martinez, P. (2018). "Continuous Monitoring and Evaluation of Cyber Security Controls in Banks." *International Journal of Banking Technology and Management*, 19(3), 231-245.

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

Huang, Y., & Nicol, D. M. (2013). A categorization of cybersecurity metrics. *ACM Computing Surveys (CSUR), 45*(1), Article 10

Johnson, M., & White, L. (2020). *Cyber Security Awareness Training: Best Practices for Banking Employees*. Publisher Name.

Jones, A., & Williams, B. (2019). *Cyber Security Risk Management in Banking: Principles and Practices*. Publisher Name.

Kannan, P. K., Rees, R., & Seetharaman, A. (2021). Cyber security risk management in the banking sector: A systematic review. *International Journal of Information Management*, 57, 102250.

Lai, V. S., & Li, H. (2005). Technology acceptance model for internet banking: An invariance analysis. *Information & Management, 42*(2), 373-386

Managing Business Risks: Strategies and Techniques. Sharma, Rajesh. (2003). ABC Publishing

Meske, C., & Stieglitz, S. (2013). Leveraging social influence for behavioral change in online communities. *Journal of Service Management Research, 3*(2), 57-67.

National Institute of Standards and Technology (NIST). (2020). *NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Research Methods for Business and Management. Sekaran, U & Bougie, Roger (2016)

Risk Management and Financial Institutions. Wiley. Hull, J. C. (2018).

Risk management practice: in the case of commercial bank of Ethiopia, Amsale Cherrnet Yohannes, June 2019

Roberts, K., Anderson, S., & Wilson, E. (2019). "Vendor Risk Management in Banking: Challenges and Solutions." *Journal of Banking Risk Management*, 12(3), 145-160.

Sood, A. K., Enbody, R. J., & Bansal, G. (2013). Advanced persistent threats: Stealthy adversaries and changing landscapes. *Network Security, 2013*(11), 5-8. doi:10.1016/S1353-4858(13)70058-8

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198.

Yao, Q., Zhu, J., Gao, F., & Zhang, X. (2019). Modeling cybersecurity investment in the supply chain with risk aversion. *Decision Support Systems, 119*, 1-11

APPENDIXI–QUESTIONNAIRE

ADDISABABAUNIVERSITYSCHOOLOFCOMMERCEM

A PROGRAM

Dear Participants, I would like to extend my deepest appreciation for your time in responding to the research questions provided below. My name is Fekadu Endrias and I'm a postgraduate student at Addis Ababa university school of commerce performing MA degree in project management. The title of my project work is Assessment of Cyber Security Risk Management Practices and Challenges: In Case of Commercial Bank of Ethiopia (CBE).

.

I believe, your experience will greatly contribute to the success of my research work. So it's with great respect that I ask you to fill this questionnaire. I also ask your kindly cooperation in answering the questions as truthfully as possible and your response will be highly confidential. This questionnaire will only be used for an academic purpose. The findings of the research will be shared to your organization when completed.

Cyber security risk management in banking is a multifaceted process aimed at identifying, assessing, mitigating, and monitoring cyber threats and vulnerabilities to protect sensitive financial data and maintain the integrity of banking operations

If you have any questions or comments, please don't hesitate to contact me.

You can reach meat;

Mobile: +251-9-13212724

Email: fekaduendrias@gmail.com

With best Regards,

Fekadu Endrias

Section B: Cyber security risk management practices

Assessing the existing cyber security risk management practices

Q.N	**Question Description**	**1 - Strongly Disagree**	**2-Disagree**	**3-Average**	**4-Agree**	**5-Strongly Agree**
1	The overall preparedness of CBE in managing cyber security risks is enough					
2	Commercial Bank's incident response procedures are effective in addressing cyber security incidents					
3	CBE has implemented best security controls (e.g., firewalls, antivirus software) to protect against cyber threats					
4	CBE provides adequate cyber security training and awareness programs to its employees					
5	CBE is highly compliant with relevant cyber security regulations and industry standards					

6	The communication and reporting mechanisms in place for cyber security incidents within CBE is satisfactory					
7	CBE invests sufficient resources in cyber security measures to adequately protect against cyber threats					
8	CBE is proactive in continuously improving its cyber security practices in response to evolving threats and vulnerabilities					

Human factors

Security Awareness and Training

Q.N	**Question Description**	**1-Strongly Disagree**	**2-Disagree**	**3-Neutral**	**4-Agree**	**5- Strongly Agree**
1	Security awareness and training programs provided by CBE is effective in enhancing your knowledge of cyber security threats and best practices					
2	I feel that the security awareness and training sessions offered by CBE have **positively influenced** my ability to identify and respond to potential cyber security risks					
3	I am **confident** in my understanding of cyber security principles and protocols after participating in the security awareness and training initiatives provided by CBE					

Behavioral Aspects

Q.N	Question Description	1	2	3	4	5
1	How **consistently** do you adhere to the cyber security policies and procedures established by CBE when performing your job responsibilities?	**Rarely**	**Occasionally**	**Sometimes**	**Often**	**Always**
2	When faced with a potential cyber security threat, **how likely** are you to promptly report it to the appropriate authorities or follow the prescribed incident response protocols?	**Very Unlikely**	**Unlikely**	**Neutral**	**Likely**	**Very Likely**
3	How well do you **prioritize** cyber security considerations in your day-to-day activities within CBE?	**Not a Priority at All**	**Low Priority**	**Neutral**	**High Priority**	**Very High Priority**

Psychological Factors

Q.N	Question Description	1	2	3	4	5
1	How **concerned** are you about the potential consequences of a cyber-security breach affecting CBE's operations and reputation?	**Not Concerned at All**	**Slightly Concerned**	**Moderately Concerned**	**Very Concerned**	**Extremely Concerned**
2	When encountering suspicious emails or websites, how **anxious** do you feel about the possibility of being targeted by cyber attackers?	**Not Anxious at All**	**Slightly Anxious**	**Moderately Anxious**	**Likely**	**Very Anxious**
3	How **confident** are you in your ability to recognize and respond effectively to cyber security threats within CBE?	**Not Confident at All**	**Slightly Confident**	**Moderately Confident**	**Very Confident**	**Extremely Confident**

Cognitive Load

Q.N	Question Description	1	2	3	4	5
1	How **mentally taxing** does you find it to comply with the cyber security protocols and guidelines while performing your job duties at CBE?	**Not at All**	**Slightly**	**Moderately**	**Very**	**Extremely**
2	How **challenging** does you find it to maintain vigilance against cyber security threats while balancing other job demands at CBE?	**Not at All**	**Slightly**	**Moderately**	**Very**	**Extremely**
3	How often do you experience cognitive overload when dealing with complex cyber security issues or incidents at CBE?	**Rarely**	**Occasionally**	**Sometimes**	**Often**	**Always**

Social Influence

Q.N	Question Description	1 -Strongly Disagree	2-Disagree	3-Neutral	4-Agree	5-Strongly Agree
1	The actions and behaviors of my colleagues influence my adherence to cyber security best practices within CBE					
2	I feel a sense of highly responsible towards promoting a culture of cyber security awareness and compliance among my colleagues at CBE?					
3	Most of the time I seek advice or guidance from your peers or supervisors regarding cyber security-related matters at CBE					

Organizational culture and leadership

Leadership Commitment

Q.N	**Question Description**	**1 -Strongly Disagree**	**2-Disagree**	**3-Neutral**	**4-Agree**	**5-Strongly Agree**
1	Senior leaderships communicate the importance of cyber security to employees?					
2	There is high rate level of senior leadership's commitment to cyber security initiatives					
3	I believe that senior leadership prioritizes cyber security within the organization?					

Security Culture

Q.N	**Question Description**	**1 -Strongly Disagree**	**2-Disagree**	**3-Neutral**	**4-Agree**	**5-Strongly Agree**
1	The overall cyber security culture towards cyber security among employees is enough					
2	Do you agree that employees understand the importance of cyber security in protecting organizational assets?					
3	Do you agree that there is comfortable environment for discussing security concerns with your colleagues?					

Communication and Collaboration

Q.N	Question Description	1 -Strongly Disagree	2-Disagree	3-Neutral	4-Agree	5-Strongly Agree
1	Departments always collaborate to address cyber security challenges					
2	CBE communicate about changes or updates to security policies and procedures					
3	There is an effective communication channel for sharing security-related information within your organization					

Effectiveness of cyber security risk management practices

Q.N	**Question Description**	**1 very ineffective**	**2-ineffective**	**3-effective**	**4-somewhat effective**	**5-very effective**
1	How effective do you find the cyber security risk process in identifying and addressing potential threats					
2	How effective are the existing technologies in cyber security risk management protecting banks asset					
3	How effective are the existing technologies in mitigating third-party risks					
4	How effective is the banks cyber security risk management in addressing emerging threats					

Challenges of implementation cyber security practices

Q.N	**Question Description**	**1 - Strongly Disagree**	**2-Disagree**	**3-Neutral**	**4-Agree**	**5-Strongly Agree**
1	There is high extent of resource constraints (e.g., budget, staffing) as a hindrance to effective implementation of cyber security measures at CBE?					
2	There are high challenging of technological complexities of implementing cyber security solutions within CBE					
3	There is a high extent of employee resistance to change poses a barrier to the successful implementation of cyber security initiatives at CBE?					
4	There are high extent of the burden of regulatory compliance impede the implementation of cyber security measures at CBE					
5	There are high concern about the risks associated with third-party vendors or suppliers who have access to Commercial Bank's systems or data					

6. Specify, if any, other challenges of cyber risk management practice faces:

APPENDIXII–INTERVIEWQUESTIONS

For Key Informants

1. What are the main challenges faced by CBE in effectively managing cyber security risks?
2. What are the methods your organization usually apply to handle challenges?
3. In your opinion what are the most non-technical factors that affect the effectiveness of cyber security management practices?
4. Can you discuss the role of organizational culture and leadership in shaping cyber security practices? How does leadership commitment influence?