ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES SCHOOL OF INFORMATION SCIENCE

IT/IS RISK MANAGEMENT FRAMEWORK FOR THE NATIONAL BANK OF ETHIOPIA.

By

Mohammed Kemal

June, 2025

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

IT/IS Risk Management Framework for the National Bank of Ethiopia.

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

Done By: Mohammed Kemal

Advisor: Temtim Asefa(Phd)

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

IT/IS Risk Management Framework for the National Bank of Ethiopia.

A Thesis Submitted to School of Graduate Studies of Addis Ababa University

in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information System

Done By: Mohammed Kemal

Name and signature of Members of the Examining Board

Temtim Asefa (PhD)	_____	_____
Advisor	Signature	Date
	_____	_____
Examiner	Signature	Date
	_____	_____
Examiner	Signature	Date

Declaration

I hereby declare that this thesis is the result of my own independent work and investigation. To the best of my knowledge and belief, it does not contain any material previously published or written by another individual, nor does it include material that has been submitted, either in whole or in part, for the award of any degree or diploma at any university or other institution of higher learning, except where proper acknowledgment is made in the acknowledgments section.

Signature:

Mohammed Kemal

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

Advisor's Signature:

Temtim Asefa (PhD)

Dedication

This thesis is dedicated to Almighty Allah, my Creator and constant source of strength, who has blessed me with inspiration, wisdom, knowledge, and guidance throughout this journey.

Acknowledgments

I begin with heartfelt gratitude to Almighty Allah, whose infinite mercy, strength, and guidance sustained me throughout this research journey, enabling me to navigate challenges and complete this thesis. My deepest appreciation extends to my advisors, Temtim Asefa (PhD), whose insightful guidance, steadfast patience, and scholarly expertise were pivotal in shaping this study. His constructive feedback and encouragement significantly enriched the development of the Information System risk management framework for the National Bank of Ethiopia. I am immensely grateful to my beloved wife, Hawi Ahmed, for her unwavering support, boundless encouragement, and steadfast belief in my potential, which provided the emotional resilience to persevere. To my cherished children, Mahir and Yusra, I owe heartfelt thanks for their patience and understanding, allowing me to dedicate time to this research despite moments when I should have been with them. Their love inspired me to strive for excellence. I extend sincere gratitude to my mother, whose lifelong encouragement and prayers have been a constant source of motivation in pursuing my academic aspirations. Finally, I would like to express my sincere gratitude to my colleagues at the NBE for their invaluable assistance with the interviews and their collaborative contributions to drafting the ISRM framework. Their practical insights and expertise were essential in grounding this research in the NBE operational context, enhancing its relevance and applicability.

Table of Contents

List of Figures

LIST OF ACRONYMS

BOD-Board of Directors

CERT- Cyber Emergency Response Team

COBIT- Control Objectives for Information and Related Technologies

CRO- Chief Risk Officer

ERM- Enterprise Risk Management

IARMD- Internal Audit and Risk Management Directorate

INSA- Information Network Security Agency

IS- Information System

IT- Information Technology

ISMD-Information System Management Directorate

ISO- International Organization for Standardization

ISRM- Information system risk management

NBE – National Bank of Ethiopia

RG- Risk Governance

RE- Risk Evaluation

RR- Risk Response

Abstract

With the increasing prevalence of cyber threats and rapid digital transformation, robust IS risk management has become essential for financial institutions particularly central banks that play a critical role in ensuring national economic stability. Despite the growing complexity and volume of IS-related risks, the National Bank of Ethiopia has not yet implemented a formal IS risk management framework aligned with its strategic objectives. The absence of a structured approach limits the bank ability to proactively identify, assess, and respond to evolving IS risks, thereby exposing critical systems to potential disruptions.

This study aims to assess the current IS risk management practices at NBE, identify organizational and procedural gaps, and propose a practical IS Risk Management Framework tailored to the institution's context. The research adopts a qualitative methodology grounded in the ISACA Risk IT Framework, focusing on the domains of Risk Governance, Risk Evaluation, and Risk Response. Data were collected through semi-structured interviews with 20 participants from ISMD, Internal audit and risk management, and business units, as well as document reviews. This study employed qualitative data analysis software (QDAS) to systematically code and interpret interview transcripts.

The findings reveal that NBE current approach to IT/IS risk management is fragmented, reactive, and poorly integrated with enterprise-level strategies. Key issues include the absence of a dedicated IS risk policy, lack of a governance committee; silos risk data, and reliance on basic risk categorization methods. Interview responses also highlighted gaps in risk communication, cross-functional coordination, and post-incident learning processes. Based on these insights and supported by international best practices (e.g., the risk IT framework, ISO 31000, COBIT 5 for Risk, and Option Based IT risk management framework), a tailored Information system Risk Management Framework is proposed. The framework includes strategic alignment mechanisms, formal governance roles, continuous risk monitoring processes, and a capacity-building agenda.

This research makes a theoretical contribution by contextualizing and extending the ISACA Risk IT Framework to the central banking sector in developing countries, addressing a gap in IS risk management literature within this underexplored domain. It provides a structured model for enhancing Information system risk oversight in NBE and similar institutions. Future studies are recommended to test the framework effectiveness across broader institutional settings and to explore quantitative validation approaches.

Keywords: IT Risk, Information system risk, the risk IT, ERM,IT governance

CHAPTER ONE
INTRODUCTION

1.1. Background of the Study

Organizations engage in various activities to achieve their objectives; however, during the execution of these activities, they may encounter a range of threats, both internal and external threats that could hinder the attainment of their goals (Sanjaya, 2015). The growing sophistication of cyber threats has significantly increased business risks, thereby positioning risk management as an essential component of organizational success (Sanjaya, 2015). These risks include operational risk, which challenges an organization's ability to achieve its strategic objectives (Deloitte, 2016); reputational risks, reflecting stakeholders' perceptions of the organization (Basel Committee on Banking Supervision, 2019); and compliance risk- defined as the potential exposure to regulatory sanctions, financial losses, or reputational damage due to failures in adhering to regulatory requirements, industry standards, or best practices (Biz, 2005). In response to the growing complexity of organizational risks, Enterprise Risk Management emerged in the 1990s as an integrated framework designed to identify, assess, and manage risks in alignment with an organization defined risk appetite (Dickinson, 2001).

Risk management plays a pivotal role in the governance of information systems, helping organizations optimize cost by preventing incidents that often require more effort to resolve than to avoid (McFadzean, 2007). However, it presents a set of challenges for both professionals and researchers. A core responsibility of risk managers is to support organizations in optimizing profitability by reducing the overall cost of risk striking a balance between the cost associated with risk mitigation and the potential losses resulting from risk realization (Lei, 2011); (Zhang, 2009). Therefore, selecting and implementing a risk management process tailored to the information systems context is crucial.

The Committee of Sponsoring Organizations (COSO, 2017) defines ERM as a strategic process, designed to provide reasonable assurance regarding the achievement of organizational objectives. Despite its comprehensive nature, ERM often overlooks information system risks, which are increasingly critical in today's digital economy (Racz, 2010). Seale (2017) emphasizes that information system risks should be explicitly integrated into ERM, as they intersect with various business risks and can trigger risks across multiple categories (Streif, 2013). (ISACA, 2016b) reinforces this perspective by emphasizing that information system risks cut across all categories of enterprise risk management (ERM), thereby necessitating integrated oversight and coordinated

response strategies. Given growing reliance on information system for organizational competitiveness and decision making, integrating Information system risk management into ERM is imperative (Rainer Jr, 2015).

The National Bank of Ethiopia, as the regulator and supervisor of the country's financial sector, plays a critical role in safeguarding macroeconomic stability, fostering financial inclusion, and promoting sustainable economic growth (NBE, 2023). To meet its strategic goals, the National Bank of Ethiopia needs to focus on strengthening the resilience of financial systems through improved risk management approaches and effective use of technology. Nevertheless, the fast pace of technological advancements and the growing intricacy of related risks present considerable obstacles. Information system risks from uncertainties in operations, potential business losses, and external factors such as political changes, increasing digitalization, and cyber threats (Kumsuprom, 2010); (Mohammad, 2014).The growing reliance on technology has further amplified these risks, making effective information system risk management essential for the Banks operational efficiency and strategic success (Damonte, 2016).

Information systems risks arise from uncertainties such as the system performance, potential business losses, and negative environmental or external factors (Seale, 2017). Information systems are not only critical for decision-making but also serve as catalysts for economic transformation (Omotayo, 2015). However, information systems are vulnerable to a range of threats that may undermine the confidentiality, integrity, availability (CIA), and accountability of the data they handle (Shukla, 2012). To address these vulnerabilities, the information systems risk management process comprising risk identification, analysis, assessment, control, and continuous monitoring is essential for effective risk mitigation (Teymouri, 2011).While multiple IS risk management frameworks exist, their heterogeneity and lack of integration often hinder effective risk governance (Wiesche., 2013). Organizations frequently adopt silos approaches to IS risk management, which, while beneficial for daily operations, fail to provide a unified framework for comprehensive risk management (Alter, 2004). Conversely, an integrated information systems risk management approach empowers executives to make well-informed decisions by harnessing synergies and systematically addressing operational IS/IT challenges (Westerman, 2007).

1.2. Statements of the problems

The National Bank of Ethiopia, as the national central monetary authority, bears a crucial mandate to ensure monetary stability and safeguard the integrity of the country financial system (NBE, 2023). In the wake of an increasingly digitalized financial ecosystem, the prominence of

information system risks ranging from cyber-attacks, data breaches and system failures poses significant threats to the operational resilience of the NBE and the broader financial sector. Business organizations annually invest hundreds of billions of dollars in technology (Barua, 1995). Technology spending worldwide is projected to reach over five trillion U.S. dollars by the end of 2025, a nearly eight percent increase on 2024 spending (Ahmed sherif, 2024). Investment in technology (exclusive of the amount spent on software) equals nearly half the spending on equipment (Zuckerman, 1994).As spending on Technology rises steeply, organizations become increasingly technology-dependent and, consequently, they become highly vulnerable to the risks of information system failure. Therefore, Information System risk-management is one of the important issues facing information systems executives today.

Ethiopia, has emerged as Africa leading target for cybercrime and is ranked as the second most attacked country globally (Sibanda, 2024).To mitigate risk management challenges, the NBE has implemented revised Bank Risk Management Guidelines (NBE., 2010), align with international standards and classify information system risks as a subset of operational risk. For instance, the March 2024 incident at the Commercial Bank of Ethiopia (CBE), where a system failure led to unauthorized withdrawals exceeding $40 million, highlights the risks financial institutions face. While such an event has not occurred at the National Bank of Ethiopia, it underscores the need for robust and specialized frameworks to address evolving technological risks (Yibeltal, 2024). Although this event was not classified as a cyber-attack, it revealed systemic vulnerabilities that demand urgent institutional attention.

International best practices offer several structured models for IS risk management, including the NIST Risk Management Framework (NIST, 2020), ISO/IEC 27001 (ISO/IEC, 2013), and ISACA Risk IT framework. While these models provide comprehensive methodologies, they often require substantial technical and financial capacity, which are often lacking in low-income countries like Ethiopia. Moreover, much of the existing academic literature tends to be predominantly theoretical, offering limited guidance on practical and scalable solutions that are specifically adapted to the unique institutional, economic, and technological contexts of such settings. This study addresses that gap by delivering a framework grounded in real-world organizational challenges**,** ensuring both relevance and applicability.

Despite the growing significance of Information Systems Risk Management (ISRM) in the financial sector, many institutions in developing countries including the National Bank of Ethiopia lack a structured, integrated, and context-specific framework for managing IS-related risks. Existing

ISRM models such as the NIST RMF, ISO/IEC 27005, and ISACA's Risk IT Framework are often developed in high-resource environments and do not always account for the institutional, regulatory, and capacity constraints present in low-income countries. Studies show that only 11.6% of Ethiopian public institutions have trial-level cyber security frameworks, while 87.4% lack any recognized standards (Adane, 2020), revealing a systemic vulnerability in national cyber resilience efforts.

This study proposes a customized Information System Risk Management Framework (ISRMF) for the National Bank of Ethiopia, built upon the principles of ISACA's Risk IT Framework. The hybrid framework incorporates structured governance mechanisms, modular adaptability, and a strong human-centered focus emphasizing employee training, behavioral analytics, and awareness initiatives. Its primary goal is to strengthen operational resilience while ensuring alignment with both national directives and international standards. Grounded in empirical evidence, case studies, and global best practices, the framework address the evolving IT/IS risk landscape at NBE and offers a transferable model for peer institutions in other developing economies.

1.3. Research Questions

1. What are the key challenges in managing information systems risks at the NBE?
2. What is the current state of information systems risk management practices at the National Bank of Ethiopia?
3. What is the essential governance, evaluation, and response processes required to develop an effective Information Systems Risk Management Framework?

1.4. General objectives

The primary objective of this research is to propose a tailored Information Systems Risk Management framework that supports the National Bank of Ethiopia in establishing an effective ITRM process one that enhances operational efficiency and strengthens the broader financial sector through improved information systems services.

1.4.1. Specific Objectives

1. To review existing Information Systems Risk Management frameworks and identify relevant best practices.
2. To assess the existing Information Systems risk management approach at the National Bank of Ethiopia.
3. To develop a context-specific Information Systems Risk Management framework tailored to the unique needs and operational environment of the National Bank of Ethiopia.

4. To evaluate the effectiveness and applicability of the proposed Information Systems Risk Management framework.

1.5. Significance of the study

This study introduces an Information Systems Risk Management (ISRM) framework specifically designed for the National Bank of Ethiopia, guided by the Risk IT framework. The proposed framework integrates principles of risk governance, strategic alignment, and enterprise-wide risk oversight (ISACA, 2009), with the goal of enhancing the Bank operational performance and ensuring its long-term resilience. Its implementation is expected to yield considerable advantages not only for the Bank but also for its personnel and the broader financial landscape in Ethiopia.

One of the core benefits for NBE is the establishment of a well-structured information system risk management (ISRM) framework that reinforces mechanisms for assessing, managing, and responding to IS-related risks. By adopting ISACA approach, the Bank can systematically identify vulnerabilities and mitigate threats, potentially decreasing the incidence of cyber security breaches and data leaks by 30–40%, a projection supported by evidence from peer organizations (ISACA, 2009).

The framework use of scenario-based analysis and well-calibrated risk appetite models enables proactive risk handling, particularly in the face of threats like phishing and infrastructure weaknesses. Integration with business continuity strategies further enhances the Bank resilience, with expected reductions in system downtime by up to 25%. This ensures that critical operations such as monetary policy execution and regulatory supervision remain uninterrupted and efficient (ISACA, 2009).

Furthermore, the framework places a strong emphasis on securing information systems and safeguarding data, which is essential to preserving public confidence in the financial system (World Economic Forum's, 2021). Aligning Information system risk practices with strategic objectives will allow the Bank to fulfill its regulatory mandates more effectively and contribute to institutional agility. Beyond institutional benefits; the framework provides structured learning and capacity-building opportunities for NBE staff. It promotes a culture of proactive risk awareness and encourages continuous learning among staff. Rooted in principles of risk ownership (ISACA, 2009), the training initiative is projected to improve staff competency in information system risk management by up to 35%, based on comparative training outcomes (Vorecol , 2024).

Moreover, workshops focusing on response techniques will prepare employees to deal more effectively with issues such as system outages and data incidents. This proactive approach is likely to reduce emergency-driven workloads, increase workplace stability, and allow staff to engage in more forward-looking initiatives. Collectively, these benefits contribute to enhanced job satisfaction and encourage professional growth through continuous learning.

On a national scale, the implementation of the framework will enhance the stability of Ethiopia financial system by improving NBE capacity to anticipate and respond to IS-related threats. Reducing such risks by 30–40% could result in significant cost savings, helping to avert cyber events that typically carry high financial consequences (World Economic Forum's, 2021). Additionally, by strengthening its supervisory capabilities, Central Banks including NBE can reinforce trust in the financial sector and support Ethiopia's broader goals for digital transformation (World Bank., 2016). The findings from this study could also serve as a reference for other regulatory institutions in sub-Saharan Africa facing similar IS risk challenges.

1.6. Scope of the study

The research scope will encompass an analysis of the current Information Systems at the National Bank of Ethiopia. This will involve evaluating the existing risk management practices and identifying potential vulnerabilities. Additionally, the research will focus on regulatory requirements, industry best practices, and the specific needs of the bank to develop a comprehensive Information Systems risk management framework. The study will also consider the organizational structure, governance, and risk appetite of the National Bank of Ethiopia.

1.7. Organizations of Thesis

This thesis is divided into six sections, and what has been discussed in each of the chapters are Highlighted in this section.

Chapter One introduces the overall paper, the background of the study, the statement of the Problem, the research purpose and questions to be answered, the scope and limitations, Justification and the significance of the study.

Chapter Two discusses and evaluate the theoretical framework and literature review. Risk concepts, and Information System risk management concepts were highlighted. It further discussed the business risk categories, the chapter concluded by literature review performed, the components have been identified and they are discussed individually. Mentioning the components in proposing

Information Systems Risk management in National Bank of Ethiopia, followed by the overall summary of the theoretical framework.

Chapter Three revealed the research methodology philosophy, design, population of the Study and sampling design. It further highlighted the data collection method, data Codification, methods, function analysis, and ethical considerations.

Chapter four present the findings of the data collected. This will form the preamble for the data analysis and discussions.

Chapter Five presented the analytical section of the study where the information from the respondent was analyzed scientifically, and data analysis and discussion, connecting it to the Literature review was highlighted.

CHAPTER TWO
Literature Review

2.1. Key Concepts

Risk is the effect of uncertainty on objectives. Effect in this case refers to deviation from the expected outcome whether positive or negative (ISO, 2009b)). Risk is established from the combination of the probability of an event and its consequence (ISACA, 2016b).

Vulnerability refers to a weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threat events (ISACA, 2016b)

Threat is anything that is capable of acting against an asset in a manner that can result in harm (ISACA, 2016b). It may also be defined threat as a potential cause of an unwanted incident (ISO/IEC 27005, 2011). A threat is therefore a set of circumstances that has the potential to cause harm.

Exposure refers to the potential loss to an area due to the occurrence of an adverse event (ISACA, 2016b). Exposure therefore refers to the extent of loss the organization has to face when a risk materializes.

Risk appetite is the broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (ISACA, 2016b).

Risk tolerance is the organization's or stakeholder's readiness to bear the risk after treatment in order to achieve its objectives (ISO, 2009b).

IS/IT Risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT (ISACA, 2009), the Risk IT Framework).IT risk is a component of the enterprise risk. All other risk categories have an IT-related component as depicted in Figure 1 e.g. a failed IT system may provide inaccurate information to management leading to an organization filing erroneous tax returns and incurring legal penalties (compliance risk).

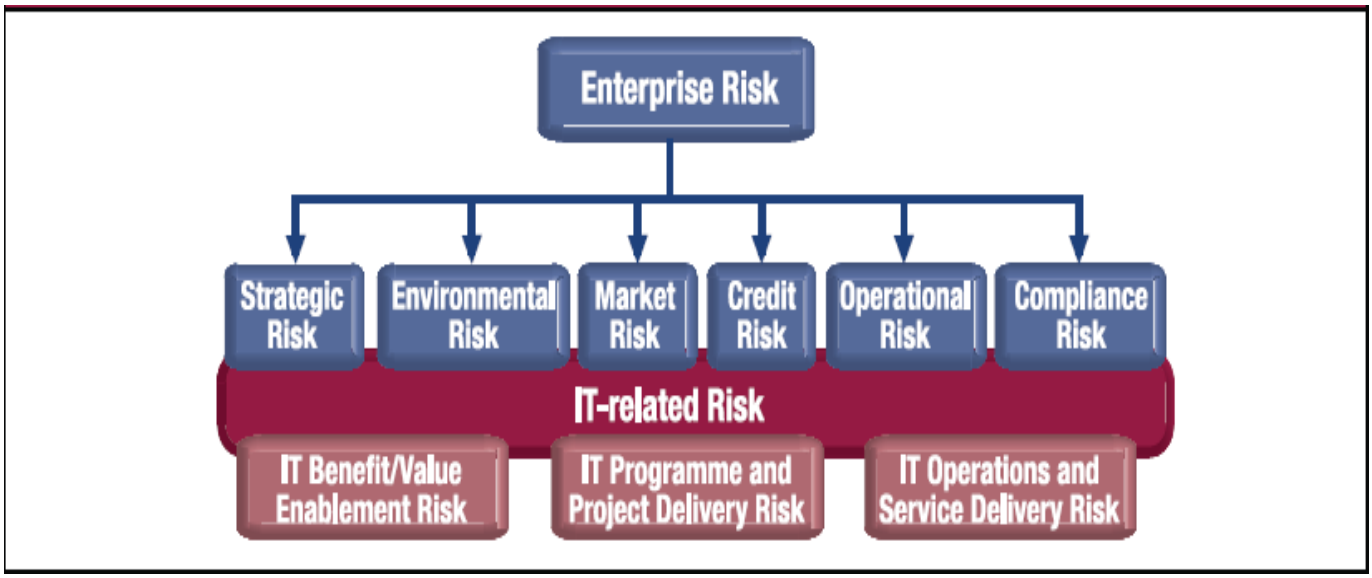


Figure 1 : IT Risk in the Risk hierarchy

Source: (ISACA, 2009), *The Risk IT Framework*

2.2. Risk Concept

Risk makes sense in every single human effort (Damodaran, 2008). It had been defined in several ways. It often carries different technical meanings in different fields and can be used in different cases, this multidisciplinary hamper us from finding some common consent in terms of its definition and utilization (Walke, 2011). Risk is an important part of individual and organizational decision-making processes and, in many situations, risk taking seems to be the only available strategy to deal with risk (Hora, 2013). The concept of risk varies according to the views, attitudes and experiences of each individual and it is affected by its own mindset (Walke, 2011). Engineers and designers look at risk from a technological perspective. Others look at it from an economic and financial point of view or from the side of environmental and health (Walke, 2011).

Risk, as a concept, has been defined in various ways by different authors and organizations, each emphasizing distinct aspects of uncertainty and its impact on objectives. According to ISO 31000, risk is the "effect of uncertainty on objectives," which encompasses both positive and negative impacts, underscoring how risk can be an opportunity as well as a threat (ISO, 2018).

(Kaplan, & Garrick, 1981) define risk as the combination of the probability of an event and its consequences, presenting a quantitative approach that is often used in risk analysis.

Similarly, (Hubbard, 2009) sees risk as the "uncertainty that matters," indicating that it is not just the uncertainty itself but its relevance to stakeholders that defines risk. In financial terms, (Hull,

2012) defines risk as exposure to adverse consequences due to uncertainty, specifically focusing on potential financial losses. (Knight, 2006) offers a distinction between "risk," where the probabilities of outcomes are known, and "uncertainty," where they are not, which has influenced much of the modern economic theory on risk. In the context of project management, the Project Management Institute (PMI) describes risk as "an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives" (PMI., 2021.), integrating both the possibility of negative and positive outcomes. In information systems, COBIT (ISACA, 2019) describes risk as the potential for events to affect the achievement of IS objectives, highlighting its relevance in technology governance. These varying definitions illustrate how risk is conceptualized differently across fields but consistently tied to the themes of uncertainty, consequences, and impact on objectives.

2.3. Business Risks Categories

Financial institutions face a wide range of risks in their day-to-day operations (Haneef, 2012). These risks include credit risk, liquidity risk, regulatory risk, and operational risk. The National Bank of Ethiopia (NBE, 2003) issued the Revised Bank Risk Management Guidelines to align with international standards and best practices. These guidelines identify key risk categories: credit, liquidity, market, and operational risks. Additionally, the Requirements for Information Technology Management of Banks (Directive No. SBB/83/2022) introduced concepts like IT risk tolerance and thresholds. Effective risk governance programs are essential to manage IS risks within defined thresholds. In banking, risk-taking is necessary, but must be understandable, measurable, controllable, and within the institution's capacity to endure losses. Although relatively underdeveloped, Ethiopia’s banking sector has experienced significant growth in recent years. This evolution requires robust risk management frameworks. (Vidalis, 2004) classifies business risks into the following categories:

2.3.1. Strategic risks

Strategic risks refer to those that affect the achievement of business objectives (Emblemsvåg, 2002). However, it was argued by (Anderson, 2020) argues that definitions of strategic risk vary based on background and professional orientation, this position is also supported by (McConnell, 2015). (Allan, 2007) views strategic risks as those that materially affect an organization’s survival, arising from uncertainties in strategic decision-making. (Roberts, 2012) assert that strategic risks tend to be more complex and difficult to assess, and it also includes risk relating to the long-term

performance of the organization. (Peter, 1997), defines strategy as a top-management plan to align actions with organizational objectives.

2.3.2. Operational risks

(Roberts, 2012) define operational risks as the risk of direct or indirect loss, resulting from inadequate or failed internal processes, people and systems or from external events. It is include events such as mistakes or missed opportunities. Operational risks are major risks that affect an organization's ability to execute its strategic plan (Deloitte, 2016). Operational risk encompasses a range of hazards, including long-standing risks such as fraud, as well as more contemporary threats like cybercrime and computer system failures (Robertson, 2016). These risks can manifest in various ways and have the potential to result in losses of any magnitude. Whether the losses are relatively minor or substantial enough to swiftly disrupt an organization, operational risks pose a significant challenge (Robertson, 2016). (Robertson, 2016) asserted that Up to now, the focus of operational risk management strategies has been on assessing historical operational risks, setting aside funds to fulfill regulatory capital standards, and, when feasible, acquiring insurance or alternative risk-transfer instruments.

2.3.3. Compliance risks

Compliance risk is defined as: "an exposure to legal penalties, financial loss and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices (Biz, 2005).Compliance risks are risks related to legal and regulatory compliance. Compliance Risk is an integral part of any organization, It involves identifying, evaluating, and mitigating potential losses stemming from the failure to adhere to laws, regulations, and standards, as well as internal and external policies and procedures (Chris, 2024). Compliance risk refers to the potential for an organization to suffer financial, legal, or reputational harm due to non-compliance with laws, regulations, and standards. Compliance risk can arise from a variety of sources, including failure to adhere to regulatory compliance obligations, inadequate training of employees, lack of oversight, and ineffective risk management strategies (Chris, 2024).

2.3.4. Financial risks

According to, (Deloitte, 2016) financial risks include areas such as: Financial reporting, Valuation, Market, Liquidity and Credit risks. (Horcher, 2005) asserts that the following are the main sources of financial risks: Organizations' exposure to changes in market prices, such as interest rates,

exchange rates, and commodity prices. Actions of, and transactions with, other organizations such as vendors, customers, and counterparties in derivatives transactions. Internal actions or failures of the organization, particularly people, processes, and systems. Financial risks of an enterprise are the result of the choice by its owners or managers of an alternative financial solution, aimed at achieving the desired target result of financial activity with the probability of incurring economic damage (financial losses) due to the uncertainty of the conditions for its implementation (Cerchiello, 2016). According to (Rick Nason, 2018) financial risk arises through countless transactions of a financial nature, including sales and purchases, investments and loans, and various other business activities.

2.3.5. Reputational risks

Reputation is often defined as public judgment of an individual or organization's qualities or skills (Martin G, 2011). Nevertheless, the interdisciplinary nature of corporate reputation as a scientific term which is repeatedly emphasized in literature has caused terminological difficulties to define corporate reputation (Chun, 2005). (Bebbington, 2008) defines reputational risk as the possibility of loss or decline/ decrease in the reputation of an organization. An organization's reputation and managing reputation are essential in today's organizations. (Basel Committee on Banking Supervision, 2019), define Reputational risk as multidimensional and reflects the perception of other market participants.

Furthermore, it exists throughout the organization and exposure to reputational risk is essentially a function of the adequacy of the bank's internal risk management processes, as well as the manner and efficiency with which management responds to external influences on bank related transactions (Basel Committee on Banking Supervision, 2019). Reputational risk is a loss in an organization's perceived trustworthiness or integrity. It has a negative impact, resulting in direct losses in revenue, indirect losses of customers, orders, employees, foregone business opportunities, or perception of the brands. Reputational loss is usually a consequence of another business risk; negative news spreads quickly and beyond the company's control.

2.3.6. Information System Risks

(Teilans, 2011), define information system risk as "the unavailability of computer software and hardware due to incidents such as denial of service attack, lack of expertise of information system personnel, loss of company's data due to theft; system malfunction or system. (Jordan, 2005) explains it as "something that can go wrong with information system and cause a negative impact on the business". The number of information system risks has increased because the technology

that carries information has evolved over the years (Damonte, 2016). Organizations that rely on information need to be aware of information system risks that may affect the operations of the organizations. With the evolving technology, information may be vulnerable to being improperly disclosed, modified, destroyed or even lost. (Kumsuprom, 2010) identifies risks such as information loss, reputational loss, business continuity failures, loss of customer trust, and loss of competitive opportunities as organizations' major information Technology- related risks.

Information system-related risks result from uncertainty around aspects such as information system operations, the probability of business losses or failure, and negative outcomes originating from both internal and external environments (Seale, 2017). However, information system risks should be managed like any other risk in the organization, and therefore, (Seale, 2017) asserts that information system risk management has become an important organizational function to control and handle risks resulting from the use of information system. (Bornman, 2008) indicates that the information system risk management does not only encompass the security of information but also includes process, financial, investment, business and any other risks that may have an impact on information technology and performing information system risk management allows the organization to better monitor information system-related risks (KPMG, 2014).The goal of IS risk management is to safeguard IT assets including data, hardware, software, personnel, and facilities from both external threats (e.g., natural disasters) and internal threats (e.g., technical failures, sabotage, unauthorized access). This ensures that potential losses from these threats are minimized (Gottfried, 1989).

Information system risk is business risk specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IS related events that could potentially impact the business. It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives. IS risk can be categorized in different ways. Common risks included in the Risk IT framework (ISACA, 2009) and similar frameworks (e.g., (COBIT 5, ISACA, 2012)) typically assessed by firms are the following: 1) IT benefit/value enablement risks associated with missed opportunities to use technology to improve the effectiveness and efficiency of business processes; 2) IT program/project delivery risks associated with quality, relevance and overrun of projects that tie into the IT investment portfolio management; and 3) IT operations and service delivery risks associated with the performance of IT systems and services such as service interruptions, compliance, and security. Since IT program/project delivery risks are conjoined with strategic and operational IT risks and

already possesses extensive research in the project management literature (Taylor, 2012), we focus our attention on the two remaining and understudied IT risk categories of benefit/value enablement risks and operations/service delivery risks.

2.3.6.1. Value enablement risk

According to ISACA Risk IT Framework, value enablement risk arises from an organization's inability to realize benefits from IS-enabled investments. This risk is often associated with poor alignment between IS strategies and business objectives, ineffective project execution, or failure to manage change effectively. ISACA emphasizes that this risk challenges organizations to not only achieve but also sustain the value derived from IT systems and investments (ISACA, 2009).

According to Ward and Peppard (2002) in their work on IT value management, describe value enablement risk as the risk of IT initiatives failing to support and enhance business performance. They argue that achieving business value from IT investments depends on strong governance, alignment with strategic objectives, and clearly defined value realization plans (Ward J and Peppard J, 2002).

According to Van Grembergen and De Haes (2009), emphasize that value enablement risk is an integral part of IT governance frameworks like COBIT. They point out that organizations face this risk when Information system fails to meet stakeholder expectations or deliver business outcomes, largely due to gaps in decision-making processes, resource allocation, or monitoring practices (Van Grembergen, 2009).

2.3.6.2. Project delivery risk

Project delivery risk pertains to the likelihood of a project failing to achieve its objectives, adhere to timelines, stay within budget, or meet quality standards (Debreceny, 2013). This risk is especially pertinent in IT programs and projects due to the inherent complexity and dynamic nature of technological initiatives. Effective management of project delivery risk is essential to ensure the successful completion of IT projects and the realization of their intended benefits (Barua, 1995).

2.3.6.3. Service delivery risk

Service delivery risk refers to the potential for an organization to fail in providing services that meet established standards, timelines, or customer expectations (Van Grembergen, 2009). This risk can arise from various factors, including inadequate resource allocation, process inefficiencies, technical failures, and external disruptions. Effective management of service delivery risk is crucial

for maintaining customer satisfaction, operational efficiency, and overall organizational performance (Debreceny, 2013).

2.4. Information System Risk Management

Risk and risk management have been extensively studied across various disciplines, including information systems, engineering, banking, insurance, economics, management, medicine, and operations research (Frame, 2003). While each field approaches risk from its domain-specific lens, all share the fundamental objective of identifying, assessing, and mitigating potential threats. Risk typically arises in situations where decisions are made with an understanding of the probability of a risk event, indicating that the decision-maker has more information available than if such probabilities were unknown (Frame, 2003). Risk, defined as a measure of the probability and magnitude of adverse effects, is inherently quantitative and must be quantified to be effectively managed. However, accurately quantifying the effectiveness of risk assessment and management in software and information assurance using a well-defined metric one that is universally applicable, replicable, and comparable has proven challenging (Frame, 2003). While significant progress has been made in quantifying various types of risk, determining the true value of risk to information integrity or infrastructure protection remains difficult (Longstaff, 2000). In essence, risk is often considered a negative outcome or event with a known or estimated probability of occurrence, based on experience or theoretical models (see, for example, (Willcocks, 1999). Raftery (1994), suggests that risk is quantifiable and can be defined as the deviation of an actual outcome from its estimated or forecasted value.

In this study, we will explore some of the risk definitions employed in these diverse fields and examine how they relate to the concept of IS risk. Information System risks are understood to arise from the potential for undesirable events that could lead to losses, threats to data privacy and security, and significant impacts on the well-being of organizations and individuals. In other words, information systems have always faced risks from malicious actions, inadvertent user errors, and both natural and man-made disasters. In recent years, these systems have become even more vulnerable due to increased interconnectivity, making them more interdependent and accessible to a larger number of individuals. Furthermore, as the number of individuals with computer skills continues to grow, intrusion or “hacking” techniques have become more widely known through the Internet and other media (GAO, 1999).

Reliable information, in regards to risks associated with information system, was produced in 2006. The report was presented by ISACA, which is an international professional association. The

association focuses on Information systems governance, providing definitions of risk management (ISACA, 2016b). In this case, risk managers are in a better position to balance economic and operational protective measures. The head of the Information systems organization must be in a position to understand that capabilities ought to accomplish its mission. Also, the national information assurance training and education center defines risk management as the process of identifying and minimizing the impacts of uncertain events. In this department, risk management aims to reduce risk as well as obtain and better still maintain approval. Besides the two, another source, managerial science, also verifies that risk management in information technology encompasses four phases. The first phrase is a management decision, effectiveness review, control implementation, and risk assessment, as received from an evaluation of threats and vulnerabilities.

The general process of risk management in information system is eliminating or minimizing uncertain events, affecting system resources (Chapman, 2011). Therefore, risk management in information system is encompassed under risk analysis, security evaluation of safeguards, implementation and test, and finally, overall security review. (Chapman, 2011)Defined risk as exposure to possible financial gains or losses. To better understand different authors, breaking it down to three stages, first approached the task of risk management. Risk analysis is the first, risk identification, the second, and risk response the third.

2.5. Information System Risk management decision making

Decision-making occurs within an environment characterized by three components: certainty, uncertainty, and risk (Flanagan, 1993). Certainty is characterized by a situation where all factors influencing a potential event are precisely identified and known to the decision-maker. In contrast, uncertainty refers to scenarios where the factors are unknown or indeterminate, making it impossible to describe the probability of the event occurring. According to Deloitte (2016), risk management tools consider whether risk is endogenous or exogenous. In Information System, risk management involves both endogenous and exogenous factors. Exogenous risks in IS include threats that originate outside the organization, such as cyber-attacks, natural disasters, or supply chain disruptions. Management strategies for these risks may involve measures like external security services, disaster recovery plans, and insurance. Endogenous risks in IS are internal to the organization and can be influenced by internal processes and decisions. These might include risks from system design flaws, user errors, or inadequate security practices. To manage these risks, IS strategies may focus on improving system architecture, implementing robust internal security protocols, conducting regular audits, and providing employee training. By addressing both types of

risks, organizations can better safeguard their IT infrastructure and ensure operational resilience (Deloitte, 2016).

2.6. Review of Existing Information System Risk Management Frameworks and Standards

To guide the development of the process model, a risk management framework was required to establish connections between observations and facts and to identify key concepts and the relationships among them.

2.6.1. International Risk IT Model

The Information Systems Audit and Control Association (ISACA) introduced the international Risk IT model, offering a holistic perspective on IT-related risks affecting businesses. According to Bakshi (2012), the fundamental premise of the Risk IT framework is that organizational leadership can effectively manage IT risks, identify potential business opportunities, and ultimately enhance returns on investment. This model serves as the foundational framework for the present study. The Risk IT model is structured into two primary components: the Risk IT Framework and the Risk IT Practitioner Guide. As noted by (D. Shaun, 2016), between 2008 and 2009, ISACA coordinated an extensive collaborative effort involving 112 professionals from 18 countries, supported by more than 1,700 IT experts. The initiative comprised seven IT risk task forces, six core development team members, 65 expert reviewers, 11 framework committee participants, and 14 board members. Risk IT was developed to address misalignment between enterprise risk management and IT risk management by equipping business leaders with comprehensive tools to assess and respond to technology-related risks. It supports decision-making processes concerning threats that impact information systems. The framework is built on three principal domains: risk governance, risk evaluation, and risk response (ISACA, 2009). IT risk may arise from a variety of sources, including service disruptions (e.g., denial-of-service attacks), deficiencies in IT personnel expertise, data breaches, or system failures and technical malfunctions (ISACA, 2009).

In another definition, ISACA characterizes Information Systems Risk Management as the safeguarding of information within an organization's technological infrastructure, aligned with its risk appetite. This includes evaluating the business impact of technology-related risks, ensuring regulatory compliance, and aligning IT functions with business objectives (ISACA, 2016b). (Debreceny, 2013) highlighted that ISACA later integrated the Risk IT framework into COBIT 5, consolidating governance and risk management efforts. Similarly, (Svatá, 2009) endorsed the Risk IT framework as highly suitable for managing IT risks, noting that it provides detailed insights and

actionable guidance for institutional leaders to effectively oversee information system risk management. This framework is aimed of encouraging the inclusion of IT risk management at the highest level of corporate decision making. This is achieved by integrating IT risk Management into the overall ERM. It provides guidelines on how to manage IT-related risk including non-technical aspects. It also provides for the communication of IT-related risks and associated controls to both IT and non-IT personnel. Cost effectiveness of controls is also taken into account to ensure that they deliver measurable value to the enterprise (ISACA, 2009). The framework consists of three domains:

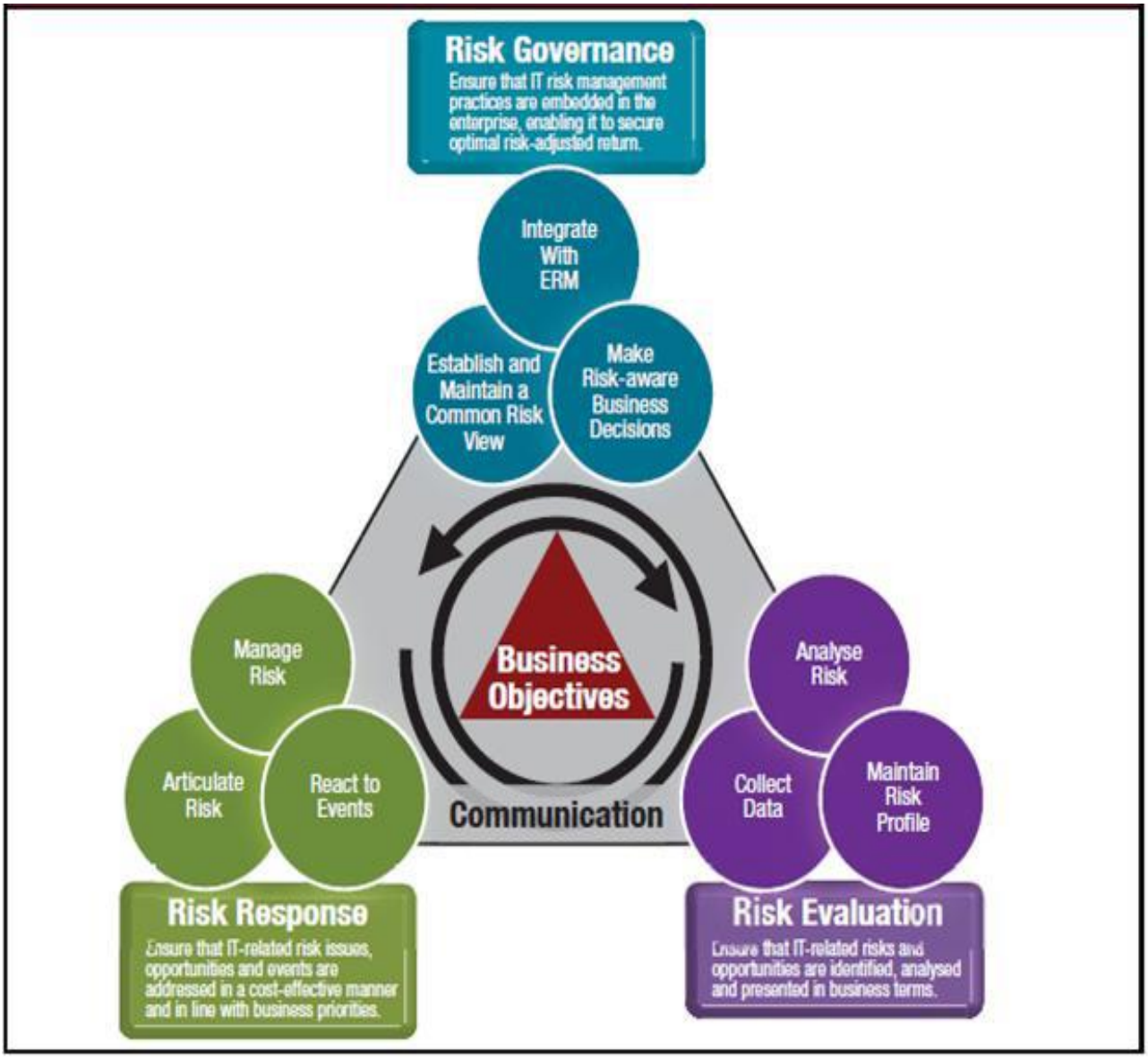


Figure 2 : Conceptual Structure of the ISACA Risk IT Framework (Version 7)

Source: Adapted from (ISACA, 2009), the Risk IT Framework.

2.6.1.1. Risk governance

Risk governance is the first of the three key constructs of the risk IT framework. ISACA noted that risk governance is the governance of IT actions to manage risks associated with technology. According to (ISACA, 2009), IT risk governance activities include (a) establishing and maintaining the institution's IT risk threshold by assessing the institution's risk appetite and tolerance, (b) establishing accountable and liable risk governance officers, and (c) providing self-governing assurances for the administration of IT risks. It ensures that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return (ISACA, 2009).

Establishing and maintaining a common risk view

A fundamental aspect of effective risk management especially in Information Systems is the establishment of a common risk view. A shared understanding of risks, their potential impacts, and appropriate mitigation strategies helps align risk management with organizational objectives and ensures consistency across units (ISACA, 2009). The complexity and diversity of risks in modern enterprises necessitate a unified perspective to avoid fragmentation and to promote comprehensive oversight. (NIST., 2012)NIST (2012), in its SP 800-30 guidelines, similarly emphasizes that a common risk view is crucial for consistent threat identification and prioritization, cautioning that fragmented approaches can significantly undermine effective mitigation efforts.

A common risk view fosters collaboration across departments and leadership, ensuring that risk identification, analysis, and response activities are integrated rather than silos. (ISACA, 2009) highlights the importance of aggregating risk information across the enterprise to provide a holistic understanding of IS risks within the broader business context, while Carcary (2012), notes that misalignment in risk perceptions often leads to gaps in controls and poor decision-making. Establishing centralized risk governance structures addresses these challenges, enabling organizations to prioritize risks based on their risk appetite and tolerance (Kaplan, 2012). Moreover, maintaining a common risk view requires regular updates to accommodate evolving IT landscapes, as advocated by ISACA (2020b) and Young (2020), who stress the importance of dynamic governance in response to rapid technological changes. This principle also aligns closely with Enterprise Risk Management frameworks, which underscore the role of leadership in fostering a risk-aware culture and harmonizing risk management strategies with long-term strategic objectives (COSO, 2017). From a technological perspective, frameworks like COBIT 2019 recommend developing enterprise-wide risk profiles and monitoring systems to consolidate and continuously update risk perspectives across the organization (ISACA, 2019).

Integrating with Enterprise Risk Management (ERM)

Integrating a common risk view with Enterprise Risk Management (ERM) frameworks enhances organizational resilience by consolidating risk management efforts across all functional units. ERM offers a structured and holistic approach to managing risks, enabling organizations to view Information Technology risks not in isolation but as integral components of broader strategic and operational risks (COSO, 2017). Fraser (2014), emphasizes that IT risks must be assessed and managed within the ERM ecosystem to ensure alignment with the organization's risk appetite, strategic goals, and performance metrics. This integration allows leadership to prioritize critical Information system risks alongside other enterprise risks, fostering a unified and strategic risk response.

The ISACA COBIT 2019 framework underscores the necessity of aligning IS risk management with ERM practices by advocating for the development of consolidated risk profiles and enterprise-wide monitoring systems that support a comprehensive risk perspective (ISACA, 2019). Similarly, (Kaplan, 2012) highlights the importance of this integration, arguing that silo-based risk management often fails to address the interdependencies between business risks. His categorization of risks into preventable, strategic, and external types complements the objectives of integrating a common risk view with Enterprise Risk Management by facilitating better alignment of IS risk appetite with overall enterprise goals. However, as (Siponen, 2009) caution, the integration of IS risk into ERM can be resource-intensive and particularly challenging for organizations that lack mature governance structures. From a technological standpoint, the rapid advancement of IS systems further necessitates embedding IT risk governance within ERM frameworks, ensuring that IT-related risks are recognized and managed as vital elements of enterprise-wide risk governance initiatives.

Make Risk-Aware Business Decisions

Making risk-aware business decisions is a cornerstone of effective enterprise risk management and significantly contributes to organizational success. It involves systematically incorporating risk considerations into strategic and operational decisions, enabling organizations to balance opportunities and risks while achieving their objectives (COSO, 2017). Embedding risk management into decision-making processes allows organizations to proactively identify potential threats and opportunities, leading to better resource allocation and enhanced resilience. According to (Fraser, 2014), integrating risk assessments across governance, strategy, and operations ensures leadership visibility into risks associated with various initiatives and enables informed decision-

making based on a clear understanding of trade-offs. Establishing a well-defined risk appetite and tolerance framework is crucial, guiding organizations in evaluating acceptable risk levels for different objectives (ISACA, 2019).

Building on this, (Kaplan, 2012) highlights the importance of differentiating between preventable, strategic, and external risks when making risk-aware decisions, noting that each type demands tailored management approaches. The ISACA COBIT 2019 framework reinforces this perspective by emphasizing the integration of risk intelligence into business decision-making, advocating the use of advanced analytics and risk monitoring tools to anticipate challenges, quantify risks, and develop contingency plans (ISACA, 2019).Similarly, (Power, 2007) stresses that clear communication channels and strong leadership commitment core to Make Risk-Aware Business Decisions are essential to embedding risk awareness across the organization. (ISACA , 2020b) recommends the use of scenario analysis and risk reporting tools, which, as (Young L, 2020) argues, help bridge the gap between technical risk data and business strategy, thereby strengthening organizational resilience. Furthermore, (COSO, 2017)underscores the importance of cultivating a risk-aware culture by training employees to consider risk implications in their roles and fostering open communication around risk issues. Together, these practices ensure that decisions are made with comprehensive risk insights, reducing uncertainty and promoting sustainable strategic growth.

2.6.1.2. Risk evaluation

Risk evaluation is the second core domain of the Risk IT Framework and entails a structured process for identifying, analyzing, and documenting IT-related risks. This domain involves several critical activities, including risk identification and assessment, impact and likelihood estimation, data collection, risk analysis, and maintaining an up-to-date risk profile to effectively manage risks over time (ISACA, 2009). These risk evaluation activities form part of the risk evaluation process areas outlined in the risk IT model. The initial phase risk identification focuses on recognizing potential events that could hinder the achievement of institutional goals. This process is often supported by formal methodologies, such as the Risk Breakdown Structure (RBS) and Risk Breakdown Matrix (RBM), which organize risks hierarchically by categories and underlying causes to facilitate systematic identification and analysis (ISACA, 2009). This involves identifying IS-related risks and opportunities and presenting them in business terms that can be understood by all stakeholders. Determining the business impact of each risk provides an objective basis for communication and risk response. (Fischer, 2011) identified the identification of relevant risks from a list of things that could go wrong as one of the biggest challenges in IS risk management.

Scenario analysis helps in tackling this challenge by providing realism in IS risk Management. Scenario analysis involves developing IT/IS risk scenarios and estimating their likelihood of occurrence as well as business impact. Scenario analysis has been identified as a centerpiece of the Risk IT framework (ISACA, 2009).

Researchers such as (Y. Liu, 2016) and (R. Mehdizadeh, 2013) used risk breakdown structure for risk identification in their studies involving construction, architectural, and engineering projects. Risk assessment involves reviewing the impact and likelihood of the occurrence of a risk. (A. Herrmann, 2013) Studied risk estimation in IT/IS and suggested that the Delphi method to estimate risk provides a more reliable estimate than other risk estimation methods. The Delphi method involves selecting a panel of experts to provide their opinions on an issue despite its difficulty, risk estimation in information system is essential in supporting management to plan and rank risk management activities or prioritize information system requirements. A risk register is a tool that captures the risk tolerance, the potential risk events, and the probability of occurrence of the risk. The risk register contains a list of threats, the probability of occurrence of these threats, and the impact of the threats. A risk register contains information such as the ranking of each identified risk, the estimated cost of the impact of the identified risk, and appropriate actions for each risk.

Collect Data

Collecting and validating data is a fundamental activity in risk management, serving as the backbone for identifying, assessing, and mitigating risks. High-quality, accurate, and relevant data enables organizations to assess the likelihood, impact, and nature of risks, thereby supporting evidence-based decision-making (Stoneburner, 2002). Both qualitative and quantitative data must be systematically gathered to ensure that risk evaluations are thorough and credible. (Stoneburner, 2002) emphasizes the need for comprehensive data on assets, threats, and vulnerabilities to inform risk assessments, a principle central to collecting data.

(ISACA, 2009) highlights that data accuracy, relevance, and timeliness are crucial for meaningful risk insights. Organizations typically collect data from a variety of internal sources such as incident logs, financial reports, and audit findings and external sources, including regulatory guidelines, industry standards, and threat intelligence feeds. This multidimensional approach ensures that assessments reflect the full scope of potential exposures.

Key risk indicators (KRIs) and key performance indicators (KPIs) are valuable tools for monitoring emerging risks and evaluating control effectiveness (Fraser, 2014). Advances in technology have

significantly enhanced data collection capabilities through Risk Management Information Systems (RMIS), data analytics platforms, and machine learning models, which improve the speed and accuracy of risk assessments (Kaplan, 2012). Furthermore, integrating Internet of Things devices and big data analytics can provide real-time risk information, especially in complex IT environments (Radanlie, 2018). However, organizations must guard against poor data quality, which can distort risk insights. (ISACA , 2020b) recommends standardized data collection protocols to maintain data integrity. Engaging stakeholders such as employees, auditors, and industry experts in data collection enriches perspectives and reduces blind spots, ultimately enhancing risk assessment reliability (COSO, 2017).

Analyze Risk

Risk analysis is a fundamental element of the risk management process, enabling organizations to assess the nature, likelihood, and potential impact of identified risks. Both qualitative and quantitative approaches are essential to this process. (ISACA, 2009) emphasizes that qualitative methods, such as risk matrices and heat maps, offer broad prioritization through subjective evaluation, while quantitative techniques, including expected loss calculations and cost-benefit analyses, facilitate precise, data-driven decisions. (ISACA , 2020b) further advocates the integration of both methods to achieve comprehensive risk assessments.

Embedding risk analysis within governance frameworks enhances its effectiveness. This includes using KRIs and scenario analysis to anticipate how risks may affect strategic and operational goals (Fraser, 2014). Tailoring risk analysis methods to the organization’s industry, risk profile, and objectives is crucial, particularly in heavily regulated sectors like banking and healthcare (Kaplan, 2012).

Despite these tools, conventional risk analysis often struggles to anticipate rare, high-impact "black swan" events (Taleb, 2007). To address this, recent studies advocate leveraging machine learning and advanced analytics for improved predictive accuracy and early risk detection (Radanlie, 2018). The COBIT 2019 framework also highlights artificial intelligence's transformative potential in processing large data sets and forecasting risks. Nevertheless, human judgment remains indispensable for contextualizing and ethically interpreting risk information, avoiding over-reliance on technology (Siponen, 2009).

Maintain Risk Profile

Maintaining a risk profile is a critical activity within the risk management lifecycle, ensuring that organizations continuously monitor, update, and assess their exposure to risks. A risk profile offers a comprehensive snapshot of the organization's risk landscape, detailing the nature, likelihood, and potential impact of identified risks (ISACA, 2009). This ongoing process enables organizations to adapt to changes in both internal and external environments, ensuring risks are managed effectively in alignment with organizational objectives.

The Risk IT Framework (2009) stresses the need for keeping the risk profile current to reflect the dynamic nature of risks. Organizations operate in constantly evolving contexts influenced by technological innovations, regulatory changes, and emerging threats. Similarly, (NIST, 2020) and (ISACA ., 2020a) advocate for continuous monitoring to adapt to emerging risks, aligning with Maintaining a risk profiles emphasis on responsiveness. Regular updates allow organizations to identify, assess, and prioritize new risks alongside existing ones, maintaining the relevance of risk assessments over time.

According to (COSO, 2017), maintaining a risk profile involves the continuous monitoring and periodic reassessment of risk data, including evaluating shifts in likelihood and impact, identifying emerging risks, and assessing the effectiveness of existing controls. A well-maintained risk profile supports proactive risk management, enabling efficient resource allocation and prioritization of mitigation strategies based on real-time insights.

Technology plays a pivotal role in maintaining risk profiles. (Fraser, 2014), highlights the use of automated risk management tools and dashboards that provide real-time visibility into risk exposure, helping organizations monitor indicators, track changes, and identify trends. Leveraging such technologies enhances the timeliness and accuracy of risk data, thereby improving decision-making and governance.

Additionally, (Kaplan, 2012) emphasizes that a dynamic risk profile must align with the organization's evolving strategic goals and risk appetite, ensuring that risk management efforts remain strategically relevant. (Young L, 2020), reinforces this by noting that risk profiles should adapt to changes in business priorities and IT infrastructure.

2.6.1.3. Risk Response

According to Kutsch (2016), Risk response is the third key construct of risk IT model. The four possible risk responses are (a) avoidance, (b) reduction, (c) sharing, and (d) acceptance. Risk

response activities include (a) implementing controls, (b) communicating lessons learnt, and (c) monitoring risks, highlighted the importance of risk response in mitigating risks. Implementing controls is a function of management in managing operations. An institution can manage operations by developing procedures, standards, policies, and systems to minimize or mitigate risks associated with any identified exposure. Study by Ellul (2013), reviewed bank-holding institutions in United States and stated that institutions with sufficient risk controls had lower tail risks and higher return on asset (ROA) compared to institutions without adequate risk controls.

Monitoring risk is an essential activity for traditional and enterprise risk management program and involves ensuring that an established risk program is active. Active monitoring of risk fosters the development of appropriate risk management strategies and procedures to mitigate against identified risks such as system failure and changing regulation are technology risks affecting institutions engaged in cloud services (Babu, 2013). Risk monitoring is part of the risk response activity and essential for information system risk management. (Anikin, 2014) evaluated information security risk assessment on telecommunication network where they have considered information, host, server, telecommunication equipment's and IT services as their asset and based on pair wise comparison of question reached on probable threat based on information security risk level. This is aimed at influencing the current scenario to ensure that the risks are maintained within the enterprise's risk appetite. An organization's options include Risk avoidance, Risk Reduction/Mitigation, Risk sharing/Transfer (transferring all or part of the risk, and Risk acceptance.

Articulate Risk

Articulating risk is a critical component of effective risk management, focusing on the clear communication of risk information to stakeholders in ways that facilitate shared understanding, informed decision-making, and strategic action (Power, 2007). Risk articulation enhances accountability and aligns risk management efforts with business objectives by ensuring a consistent interpretation of risks, their potential impacts, and appropriate response strategies across the organization (ISACA , 2020b). According to (Kaplan, 2012), communication should be tailored to the needs of different audiences, delivering technical and business-relevant insights to prevent misinterpretation and support effective governance. (Fraser, 2014) emphasizes that combining qualitative descriptions with quantitative metrics further strengthens risk communication, enabling stakeholders to evaluate risk exposure comprehensively. Moreover, frameworks such as COBIT 2019 highlight the integration of risk-related data into organizational performance metrics and

governance structures, ensuring that decision-makers remain continuously informed about emerging threats and opportunities (ISACA, 2019).

Manage Risk

Managing risk is a fundamental and cyclical process that involves identifying, assessing, mitigating, and monitoring risks to ensure alignment with organizational objectives and safeguard operations, assets, and reputation while supporting strategic growth (ISACA, 2009). This process requires implementing tailored controls to address identified vulnerabilities, with (Stoneburner, 2002)) advocating a cost-effective risk treatment approach a principle embedded in manage risk and (ISACA ., 2020a) emphasizing the additional options of risk acceptance and transfer. Managing risk must align with the organization's risk appetite and tolerance levels, selecting appropriate responses such as avoidance, reduction, acceptance, or transfer based on the likelihood and impact of risks (Fraser, 2014). (Radanlie, 2018) further proposes the use of system dynamics to optimize mitigation strategies, particularly in interconnected IT systems. However, (Siponen, 2009)caution that generic controls may fail to address context-specific risks, underlining the importance of customization to enhance effectiveness.

Moreover, effective risk management extends beyond mitigation by emphasizing continuous assessment, prioritization based on business impact, and integration into organizational governance structures (ISACA, 2019)). Frameworks such as COBIT 2019 highlight the importance of embedding risk management practices into decision-making processes to foster accountability, streamline reporting, and promote a risk-aware culture across the organization. Technological advancements, including automation tools and predictive analytics, further enhance the efficiency and responsiveness of risk management by enabling real-time monitoring of key risk indicators (Fraser, 2014). These innovations help organizations anticipate potential threats, allocate resources effectively, and maintain a proactive stance toward emerging risks.

React to events

In the domain of Information Technology Risk Management (ITRM), the concept of reacting to events encompasses both proactive and reactive strategies that organizations deploy to manage identified risk events, with effective responses being critical to mitigating adverse impacts on operations, reputation, and financial stability (ISO/IEC, 2013). Effective reaction entails not only the immediate mitigation of risks but also the implementation of long-term adjustments to the organization's risk management strategies to prevent recurrence. (ISACA, 2009) emphasizes the necessity of establishing clear incident response procedures that are closely aligned with

overarching risk management objectives. These procedures must clearly define roles, responsibilities, and compliance requirements, while the integration of lessons learned from previous incidents into future risk assessments is essential for building organizational resilience (Alberts, 2003).

Furthermore, the ability to respond effectively to risk events is foundational to enhancing organizational resilience. Continuous monitoring, proactive risk assessments, and the regular updating of risk management frameworks are critical to maintaining adaptability in the face of emerging threats (ISO/IEC 27005, 2011). (NIST, 2020) Underscores the importance of comprehensive incident response planning central to react to events while (ISACA , 2020b) highlights the need for rapid reaction mechanisms. Nevertheless, (Taleb, 2007) critiques conventional reactive approaches for their tendency to focus narrowly on known risks, advocating instead for the development of ant fragile systems capable of thriving amid unpredictability. Complementing this perspective, (Young L, 2020) stresses the importance of post-event analysis as a means to refine response strategies and further enhance the organization's adaptive capacity.

2.6.2. ISO 31000: Risk Management

This is a generic framework developed by (International Organization for Standardization, 2009) for use by organizations in developing, implementing and continuously improving the risk management process. The framework aids the organizations in incorporating risk management into the overall organization management but does not prescribe a risk management system. It consists of 5 major components:

Mandate and commitment

This is aimed at gaining commitment and endorsement right from top management. This is achieved by aligning the objectives for risk management with the business objectives of the organization. This paves way for allocation of resources and assignment of responsibilities and accountabilities.

Design of framework for managing risk

This begins with the understanding the organization and its context. A risk management policy is then established for the integration of risk management into organizational processes. Resource requirements are determined with keen interest on competence and identification of who is accountable for each aspect of risk management. Plans are also put in place for communication and reporting to stakeholders.

Implementing risk management: The processes defined in the risk management policy are rolled out in all relevant functions and processes of the organization. This should however be preceded by training and information sessions for all affected parties.

Monitoring and review of the framework: Performance measures for the risk management process are put in place and periodic reviews carried out to determine progress as well as deviation from expected outcomes. Stakeholders should also be consulted to ensure that the risk management framework remains appropriate.

Continual improvement of the framework: Information obtained from performance reviews is used to make adjustments in the process in an effort to help the organization manage risks better.

ISO also developed a process for the management of risk.

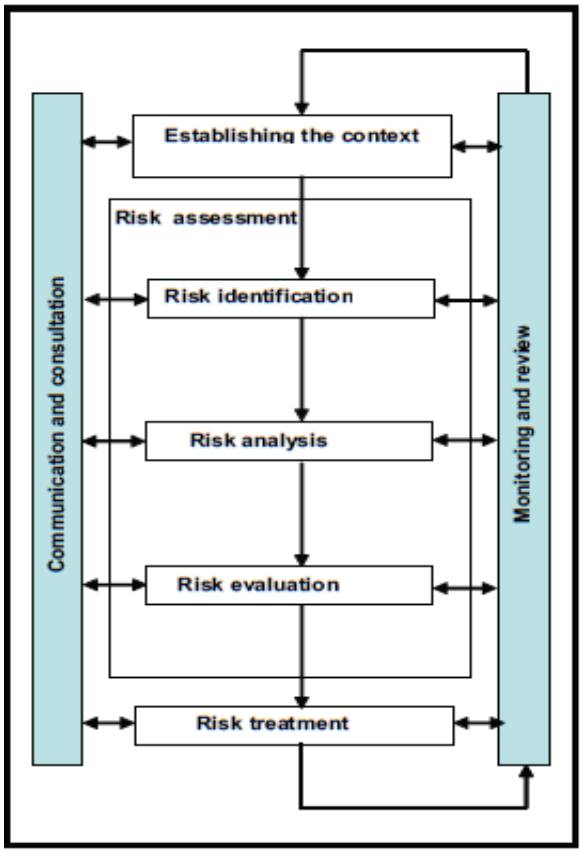


Figure 3: ISO Risk Management Process

Source: International Organization for Standardization, 2009, Risk Management - Principles and Guidelines 9

Establishing the context*:* understanding the internal and external environment. Context includes organizational culture, politics, policies, stakeholder perceptions, legal framework among other aspects.

Risk assessment*:* This is a broad area that covers identifying sources of risk, areas of impacts, causes and their potential consequences (Risk identification); developing an understanding of the risk and the factors affecting the likelihood and impact of the risk (Risk analysis) and determining if treatment is necessary based on the outcome of risk analysis (Risk evaluation).

Risk treatment*:* This covers all efforts to reduce the impact or likelihood of risk. It include weighing different options based on anticipated benefits and cost-effectiveness, planning and scheduling of actions, executing the plan, evaluating if the residual risk is within the tolerance limits of the organization as well as the relevant communication to stakeholders. Options for treatment include: transferring/sharing, avoiding the risk and accepting the risk.

Monitoring and review*:* This is aimed at establishing if the controls that have been put in place are efficient and effective as well as identifying areas of improvement. Changes in the internal and external context may also be detected and emerging risks identified.

Communication and consultation*:* At each step in the process, stakeholders should be kept informed and their views sought on their perceived performance of the process and proposals for improvement.

2.6.3. COBIT 5 for Risk

(COBIT 5, 2012) Provides a framework to guide enterprises in creating optimal value from IT by balancing the realization of benefits with the optimization of risk levels and resource utilization. The framework's control objectives for managing risk include the following steps: risk identification, impact assessment, probability assessment (likelihood of occurrence), and the development of control strategies. It encourages aligning IT risk management objectives with those of the Enterprise Risk Management framework (ISACA, 2012).

COBIT 5 for Risk builds on the COBIT 5 framework by focusing specifically on risk and providing more detailed, practical guidance for risk professionals and stakeholders across the enterprise. It also emphasizes the quantification of risk to justify mitigation costs. Moreover, COBIT 5 for Risk benefits from both internal and external stakeholder involvement, reflecting a core principle of the underlying COBIT 5 framework (ISACA, 2013).

Figure 4 summarizes the entire process.

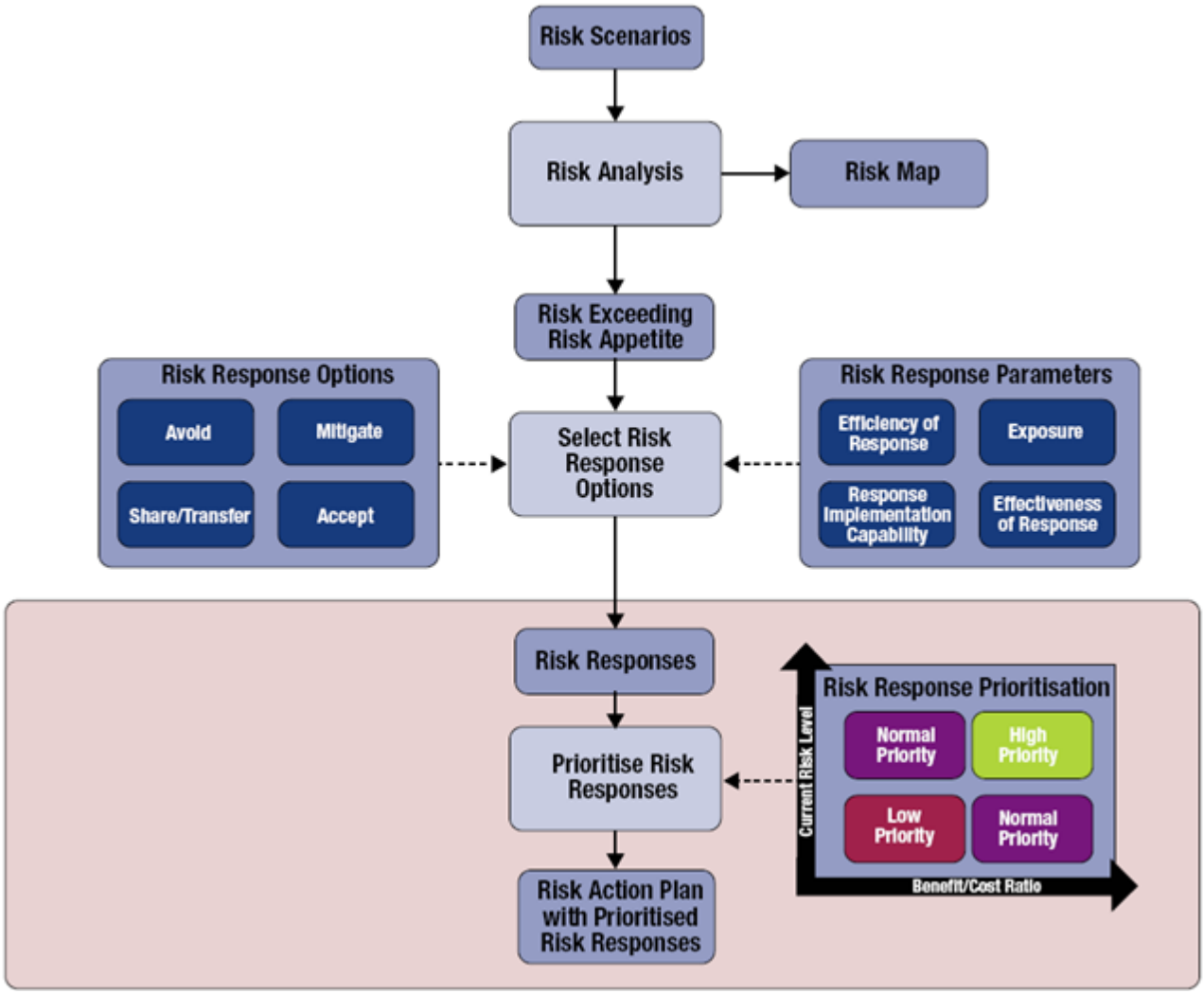


Figure 4: COBIT Risk Management Process

Source: ISACA (2013), COBIT 5 for Risk

Risk scenarios are identified and defined using either a top-down or bottom-up approach. The top-down approach begins with the overall business objectives and analyzes the most relevant and probable information system risk scenarios affecting these objectives. Conversely, the bottom-up approach starts with a generic list of scenarios, which is then refined into more concrete and customized scenarios tailored to the specific enterprise context. Risk analysis is conducted to assess the potential impact and likelihood of each identified risk. Risk response options are selected from generic categories: avoid, mitigate, accept, and share/transfer. This selection considers various parameters associated with each option, including efficiency, effectiveness, implementation capability, and the level of risk exposure. The current risk level and the expected benefit-cost ratio

are used to prioritize the risk responses. Finally, an action plan is generated from the prioritized risk responses for implementation.

2.6.4. Option Based IT Risk Management Framework

This framework assists managers in embedding various options within IT investments to effectively manage the associated risks. The framework addresses two major challenges in IT/IS risk management: adopting an economic perspective on risk management and selecting and combining appropriate mitigation strategies to effectively address specific risks (Barrenechea. M, 2013).

The framework is based on the premise that, to maximize IT investment value, a manager should assess relevant risks, incorporate sufficient flexibility into the investment to add value, and continuously evaluate new information to take corrective actions within the flexibility bounds. Option Based IT Risk Management Framework formalizes this concept by treating real options as high-level risk mitigation strategies that create the necessary flexibility to implement corrective actions when risks materialize. It facilitates identifying the combination of options that maximizes value relative to the risks specific to a particular investment. Barrenechea (2013), developed an option-based approach to managing IT investment risk, comprising the following steps:

Define the investment and its risks: Specify the investment objectives and resource requirements for the initially identified solution.

Recognize shadow options: Identify embedded options that can control the identified risks; for example, technological risks can be managed through defer, lease, and abandon options.

Design alternative investment configurations: Develop alternative configurations by combining different subsets of shadow options and assess the associated risk trade-offs.

Evaluate options and investment configurations: Select the configuration that offers the greatest value based on the evaluation.

2.7. Theoretical framework

2.7.1. Framework Selection

Based on the literature reviewed, the Risk IT framework was selected as the foundation for this study for several key reasons. In contrast to COBIT, which primarily focuses on the mechanisms for managing information systems risk through a set of controls, the Risk IT Framework emphasizes

the objectives by supporting the identification, governance, and management of IT risk. Similar to ISO 31000 and COBIT, the Risk IT Framework covers the identification, assessment, and response to IT risks. Moreover, it aligns information systems risk management with broader business objectives rather than focusing narrowly on IT assets, thereby ensuring a strategic perspective. The framework is notable for providing specific processes dedicated to governing information systems risk. It incorporates risk scenario generation techniques that facilitate stakeholder understanding and engagement with identified risks, thereby promoting broader participation. Furthermore, the framework incorporates mechanisms for the continuous monitoring of information systems risk and integrates risk management into operational processes, ensuring it remains a continuous and iterative activity (ISACA, 2009).

The adoption of the Risk IT Framework provides several key benefits for organizations aiming to improve their information system risk management practices. First, it establishes a common language that facilitates effective communication among business, IT, risk, and audit management teams. This shared terminology ensures that all stakeholders clearly understand IT risk-related concepts and processes (ISACA, 2009). Second, the framework provides comprehensive guidance on managing information systems-related risks, including identification, assessment, mitigation, and monitoring. This holistic approach enables organizations to develop a complete risk profile, allowing for a better understanding of potential risks and more efficient utilization of enterprise resources (ISACA, 2009).

Additionally, the Risk IT Framework clarifies roles and responsibilities in information systems risk management, ensuring that all relevant parties understand their duties and accountabilities. This alignment with Enterprise Risk Management (ERM) practices further integrates IT risk management into the broader organizational risk management strategy (ISACA, 2009). The framework also offers enhanced visibility into information system-related risks and their financial implications, enabling organizations to make informed decisions and allocate resources effectively. By implementing the Risk IT Framework, organizations can reduce operational disruptions and failures through proactive risk identification and management (ISACA, 2009). Moreover, the framework enhances information quality by promoting consistent and accurate risk reporting and documentation. This, in turn, enhances stakeholder confidence and mitigates regulatory risks, as the organization demonstrates a robust approach to information systems risk management (ISACA, 2009).

2.7.1.1. The Risk IT Principles

Risk IT is founded on several guiding principles for the effective management of IT risk. These principles are adapted from widely accepted ERM principles and applied specifically to the IT domain. The Risk IT Framework addresses information systems risk, that is, business risk related to the use of information systems. Its connection to business is established through the principles on which the framework is built, namely, effective enterprise governance and management of information systems risk, as illustrated in the figure below:

- Always align risk management activities with business objectives.
- Integrate the management of information systems-related business risks with the overall enterprise risk management (ERM) framework, where applicable.
- Balance the costs and benefits associated with managing information systems risks.
- Promote transparent and open communication regarding information systems risks.
- Establish appropriate tone at the top by defining and enforcing personal accountability for operating within clearly defined risk tolerance levels.
- Ensure that risk management is an ongoing process embedded in daily organizational activities.

2.8. Challenges in Managing IT Risks

2.8.1. Internal Challenges

2.8.1.1. Lack of Skilled Personnel

The World Economic Foroum (2020), highlights a global shortage of skilled professionals in emerging technologies such as cyber security, artificial intelligence (AI), blocks chain, and data analytics. This shortage is particularly acute in developing economies, including Ethiopia. The report indicates that Ethiopia's digital transformation efforts are significantly impeded by a lack of local expertise, which weakens IT security practices and delays the development of robust risk management frameworks. These findings corroborate concerns regarding the shortage of skilled information system professionals and risk managers at the National Bank of Ethiopia .

Similarly, (Kaspersky, 2023), notes Ethiopia's limited cyber security capabilities, with local firms and government agencies including the NBE often relying on costly external contractors due to a shortage of qualified personnel. This observation aligns with challenges of insufficient internal expertise in managing information system risks at the NBE. This further aligns with the challenge of insufficient internal expertise in managing information system risks at the NBE. Furthermore, the

(IMF, 2020), discusses the capacity constraints in Ethiopia's financial sector, highlighting limited human resource capacity in regulatory and supervisory roles at the NBE. The report stresses that efforts to modernize banking supervision are hampered by a shortage of trained staff, particularly in critical areas such as financial soundness indicators (FSIs) and risk assessment. This skills gap also affects information system risk management, where specialized knowledge in cyber security and data analytics is essential (IMF, 2020).

2.8.1.2. Poor Integration of IT Risk Management with Business Objectives

The NBE regulatory guidelines emphasize the importance of integrating information system risk management with broader organizational objectives to ensure financial stability (NBE., 2010). However, the guidelines also acknowledge ongoing difficulties in achieving cross-departmental coordination, particularly in resource-constrained environments like Ethiopia. Fragmented risk management processes and departmental silos significantly hinder alignment between information system risk management and business objectives. The World Bank further reports that the NBE suffers from inadequate regulatory frameworks and weak integration of risk management practices, including IT risk, into its strategic planning. Information system risk management is often treated as an isolated function rather than as part of an enterprise-wide risk management approach, which impairs the institution's capacity to address systemic risks effectively (world Bank, 2024).

2.8.1.3. Lack of Clear Policies and Procedures

The NBE own guidelines recognize that many Ethiopian financial institutions, including the NBE itself, lack well-defined information system risk management policies, leading to inconsistent practices and heightened vulnerabilities (NBE., 2010). Although the guidelines call for standardized procedures for risk identification, assessment, and mitigation, implementation remains inconsistent due to limited institutional capacity and vague procedural frameworks.

Degu, Keshav and Monika (2024), highlights the low levels of disclosure and reporting among Ethiopian banks, attributing this to the absence of clear policies and procedures. This deficiency extends to Information system risk management, where ambiguous guidelines lead to inconsistent risk mitigation strategies and increased exposure to vulnerabilities such as inadequate cyber security measures.

Similarly, The African Development Bank (2022), identifies the lack of clear information system risk management policies as a key challenge for Ethiopia's financial sector. It emphasizes that the absence of specific information system risk management guidelines contributes to reactive rather

than proactive responses to emerging threats, thus increasing the risk of system failures and cyber-attacks.

2.8.2. External Challenges

2.8.2.1. Cyber Threats

Tadesse (2024), examines the cyber security challenges confronting Ethiopian banks, including the National Bank of Ethiopia, amid escalating threats such as phishing and ransomware attacks. The study highlights a rising frequency of cyber-attacks coinciding with the expansion of internet services, while banks' capacities to implement proactive cyber security measures remain limited. To address these persistent threats, (Tadesse, 2024)recommends the adoption of multi-layered security controls and regular vulnerability assessments, emphasizing increased exposure due to its reliance on digital platforms.

The Bank for International Settlements (2023), underscores the global rise in cyber-attacks on financial institutions, including central banks, and highlights their potential to cause systemic disruptions. The report specifically points out that developing countries like Ethiopia are particularly vulnerable due to limited cyber security infrastructures, leaving institutions like the NBE exposed to operational and reputational risks.

2.8.2.2. Regulatory Changes

The European Central Bank Supervision (2024), overview of the Digital Operational Resilience Act (DORA) highlights the complexity and resource intensity of adapting to evolving cyber security regulations. Central banks in developing countries, including the NBE, face significant challenges in aligning with such international standards, particularly given their limited regulatory capacity. DORA's stringent requirements for enhancing IT/IS risk management demand significant investments in technology and expertise, which are difficult for the NBE to meet.

Similarly, the NBE own guidelines acknowledge the challenge of adapting to both domestic and international regulatory requirements, citing limited resources and institutional capacity as major obstacles (NBE., 2010). Compliance with emerging cyber security regulations often requires substantial updates to IT infrastructure and policies, putting additional strain on the NBE's already limited budget.

The (world Bank, 2024), further stresses that the NBE struggles to modernize its regulatory framework in order to meet international standards. It emphasizes that outdated regulatory

structures hinder compliance with global cyber security and risk management standards, requiring significant investments in capacity building, technological upgrades, and institutional reforms.

2.8.2.3. **Increasing Digitalization and Fintech Innovations**

The Policy Studies Institute (2024), reports that the rapid growth of digitalization and fintech innovations such as mobile money platforms and digital payment systems has outpaced the NBE's risk management and regulatory capacities. Infrastructure deficiencies, including poor internet connectivity and cyber security gaps, are major barriers to the secure adoption of fintech innovations. As a result, the NBE struggles to regulate emerging platforms like Telebirr, exposing the financial system to increased cyber threats and fraud risks.

Similarly, a World Bank blog post (World Bank, (2024), highlights Ethiopia's push toward digital financial services, noting that the NBE outdated infrastructure and limited expertise hinder its ability to oversee and secure these innovations. Poor connectivity, low digital literacy, and inadequate cybersecurity measures further exacerbate the IT risks associated with rapid digitalization, complicating the NBE's efforts to ensure financial sector stability.

2.9. Related work

In the field of information system risk management, several researchers have made significant contributions by exploring various dimensions of risk governance and management. For instance Carcary (2012), in his work titled "IT Risk Governance: Building a Risk-Aware Culture," aimed to examine how IT risk governance can be effectively structured within organizations. His research emphasizes the critical need for fostering a risk-aware culture, where IT risks are not managed in isolation but are instead aligned closely with the broader business strategy. Carcary (2012), findings indicate that effective IT risk governance requires both robust risk management processes and an organizational commitment to integrating risk awareness into routine decision-making. This alignment helps ensure that IT risk management is not merely a technical exercise but is embedded in the overall strategic objectives of the business. (Carcary, 2012) study underlines that without this cultural shift, IT risk management frameworks may fail to address the broader organizational impacts of IT risks.A (Institute of risk management, 2010) developed a risk management process based on ISO 31000 with the following components:

Risk assessment - It begins with the identification of the factors that are most critical to the achievement of the organization's objectives. These are defined in terms of opportunities and

threats. The risks are then ordered in terms of priority and this is used to determine the resource allocation for risk treatment.

Risk treatment - This involves identifying and implementing controls to reduce the impact or eliminate the risk. Approaches for risk treatment include: risk avoidance and risk transfer. The cost of risk treatment should always be compared to the anticipated benefit to ensure a net gain. Controls with the highest net gain should be given highest priority.

Feedback mechanisms - This involves monitoring and reviewing of the organization's performance as well as that of individual components. It is also important to maintain communication amongst stakeholders on issues affecting their areas of interest.

The National Stock Exchange of India Limited implemented IT risk with an aim of risk assessment into IT operational and governance processes as described by (Bakshi, 2012) .

A comparative study of existing standards and frameworks was carried to identify the most suitable guiding framework for the process. The Risk IT framework was selected for the following reasons: It provides granular guidance on risk management processes covering all traditional risk management processes (identification, risk assessment, risk response, risk treatment and risk monitoring);It focuses on linking IT risk with business objectives rather than IT assets; It is the only framework that provides detailed processes for IT risk governance; It is focused on building risk scenarios (also provide list of generic scenarios) that help in directly linking risk management with business processes. The implementation of risk management involved development of risk registers for business functions and defining an aggregation process to arrive at an organization-level risk profile. The Risk IT framework enabled the National Stock Exchange of India Limited to present a unified view of IT risks to stakeholders. It facilitated participation through scenario analysis, established a continuous process for monitoring the risk profile, and promoted acceptance by risk owners. An Excel-based tool was developed for updating the risk profile (MetLife, 2010). leveraged the Risk IT framework to create a MetLife-specific IT Risk Management Framework. They customized it to a framework that used internal terminology to ensure the document could be easily understood and used globally across the enterprise. The customized framework provides for the consistent handling of all IT risk management aspects and integrating them with business operational risk activities. It is not a procedure, but rather a description of what processes and activities management should strive to mature. It maintains the Risk IT domains (risk governance,

risk evaluation and risk response) and also provides details on the processes and activities to be carried out (MetLife, 2010).

Aven (2014), in his paper titled "Risk Assessment and Risk Management: Review of Recent Advances," aimed to review and synthesize modern approaches to risk assessment and management, with a particular focus on their application within IS and operational contexts. His objectives centered around understanding how contemporary techniques could improve the handling of uncertainties inherent in risk assessments, which are critical for effective decision-making in complex IS environments. Aven findings highlight the emergence of advanced methodologies that enable organizations to better quantify and manage uncertainties, going beyond traditional risk management frameworks. He emphasizes that addressing uncertainties is essential in operational settings, where the dynamics of IS systems and the rapid pace of technological change make risk assessment more challenging. His research underscores the need for adopting more flexible and robust approaches in IS risk management, capable of adapting to evolving threats and uncertainties.

Huang (2015), in the paper titled "Integrating Enterprise Risk Management and IT Systems," aimed to explore how Enterprise Risk Management could be integrated into IT systems to improve decision-making processes. The study's objective was to investigate how this integration could lead to more effective risk management by providing organizations with a comprehensive understanding of their risk landscape. findings demonstrate that integrating ERM into IT systems enhances system resilience and provides a more comprehensive view of organizational risk. This integration allows organizations to make more informed decisions, as they are better equipped to identify, assess, and respond to risks across both IT and business functions. Huang's work underscores the importance of a unified approach to risk management, where risk information system is not silos but aligned with overall enterprise risk strategies.

Gerrard (2017), in his study titled "The Role of IT Risk Management in Financial Institutions," sought to assess how IT risk management contributes to enhancing financial stability within the banking sector. The primary objective of the research was to evaluate the effectiveness of proactive IT risk management practices in mitigating risks that could impact financial stability. Gerrard's findings revealed that implementing robust IT risk management strategies significantly reduces the incidence of data breaches and associated financial losses. His study underscores the importance of proactive risk management in safeguarding financial institutions against potential IT-related threats,

demonstrating that effective management practices are crucial for maintaining both operational integrity and financial stability.

The NIST (2018), Publication ″NIST SP 800-37: Risk Management Framework for Information Systems" provides a comprehensive framework designed to guide organizations in assessing and managing IT risks. The primary objective of this framework is to offer a structured approach for implementing effective risk management practices across various information systems. NIST's findings emphasize the critical importance of continuous monitoring and adaptive controls as integral components of an effective IT risk management strategy. By advocating for an ongoing assessment of risks and the flexibility to adjust controls as needed, the framework ensures that organizations can respond dynamically to emerging threats and vulnerabilities. This approach underscores the necessity for vigilance and adaptability in managing IT risks, aligning with the broader goal of maintaining robust and resilient information systems.

In the study titled "Cyber Security Risk Assessment in Financial Institutions" by (Khatibi, 2020), the objective was to explore the cyber security risks faced by financial institutions and to develop a comprehensive assessment framework. The research underscores the growing significance of cyber security risk management as a critical component in safeguarding sensitive financial data. Khatibi's findings highlight that, given the escalating threats in the digital landscape, a robust cyber security risk assessment framework is essential for effectively protecting financial institutions from data breaches and cyber-attacks. The specific gap addressed by this study lies in the lack of contextualized frameworks tailored to the operational realities of central banks in low-income countries, such as Ethiopia.

Most existing works focus on global standards like NIST RMF, ISO/IEC 27005, and ISACA Risk IT Framework, which are often designed with the assumption of mature governance structures, strong technical capacities, and high levels of institutional readiness. These conditions are not always present in developing economies, where ISRM practices are often fragmented, under-resourced, or externally driven. Moreover, limited empirical research is available that examines the actual ISRM practices of central banks in such settings or proposes frameworks grounded in local institutional contexts. As such, this study contributes to the literature by bridging the gap between theory and practice, offering a tailored ISRM framework for the National Bank of Ethiopia that reflects both global best practices and national-level implementation constraints. This research therefore fills an important niche by responding to the need for locally adaptable, evidence-based frameworks, which is underrepresented in current ISRM scholarship.

CHAPTER THREE
RESEARCH DESIGN AND METHODOLOGY

This chapter outlines the research design and methodology employed to achieve the objectives of the study. It presents the research approach and techniques used to address the research questions. Additionally, the chapter discusses data collection procedures, sources of data, and considerations related to validity, reliability, and data analysis.

3.1. Research Design

This study adopts a qualitative and exploratory approach to examine the current practices of information system risk management at the National Bank of Ethiopia. A case study strategy is employed to achieve the research objectives. Qualitative research is particularly suited for studies with small sample sizes, where outcomes are not intended to be statistically measurable or generalizable. Its primary advantage, distinguishing it from quantitative research, lies in its ability to provide a comprehensive and detailed understanding of the research subject without limiting the scope of inquiry or restricting participants' responses(Collins, 2003).

In qualitative research, the researcher plays a central role in data collection and analysis, unlike quantitative research, which often relies on standardized instruments such as surveys or tests. This method frequently involves fieldwork, requiring direct engagement with the research setting through observations and interviews with relevant participants. It typically follows an inductive logic, especially when existing theories are insufficient to fully explain the phenomenon under study. Moreover, qualitative research emphasizes understanding processes through rich, detailed descriptions that contribute to knowledge construction.

However, the success of qualitative research depends largely on the researcher’s skills and abilities. Its findings are often considered subjective, as they are shaped by personal interpretations and judgments. Furthermore, due to generally small sample sizes, there is a risk that the findings may not be representative of a broader population (Bryman, 2004).

3.2. Research Approach

This study employs an inductive research approach, beginning with specific observations to develop generalized theories and conclusions. This approach is particularly suited to qualitative research, especially when working with small sample sizes, as it allows for an in-depth exploration of phenomena within their natural context. The inductive method is beneficial when existing theories

do not adequately explain the phenomenon under investigation, enabling the researcher to generate new theoretical insights grounded in empirical data.

A limitation of the inductive approach is its reliance on a limited number of observations, which may affect the generalizability and reliability of the findings (Denzin, 1970). The conclusions drawn are context-specific and may not be broadly applicable. Nevertheless, qualitative research prioritizes depth and richness of understanding over statistical generalization, focusing on the nuances and complexities of the cases studied.

3.3. Data Collection Method

This study employed a triangulation of qualitative data collection methods: face-to-face semi-structured interviews, document review, and observation, to gain a comprehensive understanding of information system risk management practices at the National Bank of Ethiopia (NBE). Triangulation enhances the depth and validity of qualitative research by integrating multiple data sources, providing richer and more nuanced insights into the research subject.

Among these methods, semi-structured interviews were pivotal. They are widely regarded as a cornerstone of case study research due to their capacity to elicit detailed, context-rich data through open-ended questions (K.Yin, 2018). This approach enables participants to express their experiences and perspectives in their own words, facilitating a deeper understanding of complex issues. The interview guide was adapted from the international Risk IT Framework, ensuring alignment with established best practices in information system risk management.

Following the interviews, internal documents were requested from participants to corroborate and enrich the interview data. Document review is a critical method in case study research, providing additional perspectives and enabling cross-referencing and validation of information obtained through interviews (Hirschhein, 2003).

Observation was also conducted to capture real-time data on NBE information system risk management practices. This method allows researchers to gather information on behaviors and interactions within their natural context, offering insights that may not be accessible through interviews or documents alone. By integrating these qualitative methods, the study aimed to develop a comprehensive and contextually grounded information system risk management framework tailored to the specific needs and circumstances of the NBE.

3.3.1. Semi Structured interviews

Qualitative interviews are widely recognized as an effective data collection method in qualitative research (Newman., 2007). They allow researchers to explore phenomena from participants' perspectives and to understand the reasons and contexts underlying these viewpoints (Cassell, 2004). To achieve this objective, the interviews were guided by open-ended questions, minimal structural constraints, and an emphasis on participants' specific experiences and situations. Face-to-face semi-structured interviews were conducted to explore the perspectives of key organizational representatives on information system risk management, as this approach provides the flexibility required to adapt to participants' responses during the interview. According to Bryman (2004), the flexibility inherent in semi-structured interviews enables researchers to explore how interviewees frame and interpret issues and events, thereby gaining insights into what they perceive as important in explaining behaviors and patterns. Complementing this, (Babbie, 1998) argues that in-depth, face-to-face interviews allow participants to guide the conversation to some extent, while adhering to a predetermined set of questions, thereby enriching the depth and authenticity of responses.

Unlike structured or entirely unstructured interviews, the semi-structured format provides both the flexibility to pursue emergent, salient topics and a consistent framework for comparing responses (Bryman, 2004). This approach supports the study's objective to capture both generalized patterns and specific organizational viewpoints. To facilitate the interviews, an interview guide containing key questions was developed, (Patton, 2002) recommendation to enable deeper probing into the subject matter.

Two versions of the interview guide were prepared, tailored to two categories of participants: IT Units and Business Units stakeholders (refer to Appendices I-II). Face-to-face interviews were employed as the primary mode of data collection, with all interviews conducted in person. The independence of the respondents, each representing distinct groups, added supplementary value to the data by ensuring diverse and unbiased perspectives.

However, as (Flick, 2002), cautions, this approach risks respondents diverting discussions toward internal organizational problems or blurring the lines between personal and professional insights. To mitigate such risks, interviewers consistently steered the conversation back to the research questions outlined in the interview guide. For respondents less formally connected to the researcher, a more relaxed conversational approach was employed to encourage openness. Each interview was scheduled for approximately 80 minutes; however, actual durations ranged from 40 to 60 minutes, with most lasting between 40 and 50 minutes. Conversations were recorded with participants'

consent and subsequently transcribed. In addition, short notes were taken during interviews for validation purposes.

3.3.2. Document Analysis

This study employed document analysis by reviewing internal documents from the National Bank of Ethiopia (NBE), including Bank Risk Management Guidelines, policies, risk assessment reports, strategic plans, and relevant banking and IT laws and regulations in Ethiopia. This method will help understand formal structures and processes, aligning with the scope to evaluate existing practices and identify vulnerabilities. To develop a comprehensive understanding of information systems risk management and to contextualize international practices in mitigating such risks, a document analysis was undertaken. This method entailed a systematic review of diverse sources, including scholarly books, peer-reviewed journal articles, conference proceedings, and reputable online resources. These materials provided critical insights into prevailing theories, methodologies, and global experiences in managing information systems risks. Notably, literature reviews such as those by (Amraoui, 2019), and comprehensive analyses in journals like MDPI's Electronics have been instrumental in elucidating the multifaceted nature of risk management in information systems.

In addition to external literature, an in-depth examination of the bank's internal risk management guidelines was conducted. This internal document analysis aimed to assess the organization's existing risk management framework, policies, and procedures. By scrutinizing these internal documents, the study sought to identify the alignment between the bank's practices and established international standards, such as those outlined in the Basel Committee's principles for effective risk data aggregation and risk reporting.

The document analysis process was pivotal in gathering pertinent information, enabling a Comprehensive understanding of both theoretical constructs and practical applications of risk management. This dual approach enriched the researcher's knowledge base, facilitating a more robust analysis of the subject matter and contributing to the study's overall rigor.

3.4.Data Source

The method of purposive sampling was used to identify the data source of this research. Purposive sampling belongs to the category of non-probability sampling techniques, sample members were selected on the basis of their knowledge, relationships and expertise regarding a research subject (K.Yin, 2018).The target population of this research was IT staffs, Internal Audit and Risk management department, and Business Units, who were working at National Bank of

Ethiopia head office. But for this specific research, the researcher identified the participants based on their current role, which was related to the issue of this research. Hence, the participants of this research for in person interview were from different ISMD and IARMD including ISMD Directors, Chief Database Administration officer, Chief IT security officer, Senior application management Officers, Chief IT infrastructure officer, Acting Chief IT supervision Officers, Senior Risk Management Officers, and Chief Risk manager of bank. Participants from Business department were includes Team leader 1 from PSSD, Senior currency management directorate, and senior finance Management directorate.

3.5. Evaluation of the Proposed Framework

To ensure the validity, applicability, and contextual relevance of the proposed IT Risk Management Framework for the National Bank of Ethiopia (NBE), a systematic evaluation process was conducted. This process employed two qualitative validation techniques: expert review to assess the framework comprehensiveness, practical utility, and alignment with both international standards and institutional requirements.

Rather than relying on statistical measures, the validation of the proposed framework was based on subjective expert judgment**,** grounded in professional experience and contextual understanding. To ensure methodological rigor, several qualitative validation tools and techniques were employed. First, an expert review was conducted, in which a group of carefully selected subject matter experts evaluated the framework against predefined criteria, including relevance, comprehensiveness, clarity, and alignment with internationally recognized standards such as the ISACA Risk IT Framework and ISO 31000. These experts were identified through purposive sampling**,** guided by eligibility criteria such as professional qualifications, active involvement in risk governance, and familiarity with IT risk management standards. Their feedback was subjected to qualitative content analysis to identify common patterns, critiques, and recommendations, which were then used to refine the framework and enhance its contextual applicability. Furthermore, expert evaluations were structured around four key validation dimensions: relevance to the organizational context, practical feasibility, clarity of framework components, and alignment with global best practices. This structured, expert-driven approach contributed significantly to the trustworthiness and practical relevance of the final framework.

3.6. Method of Data Analysis

Qualitative content analysis was employed to systematically examine data collected through semi-structured interviews and document reviews. This method was selected for its suitability in exploring complex, context-dependent phenomena such as IT risk management practices and perceptions within a central banking environment. Although numerous studies exist in the domain of Information Systems Risk Management (ISRM), the majority focus on generalized frameworks, policy-level recommendations, or quantitative metrics applied in different institutional or geographic contexts. However, this study specifically aims to explore the current ISRM practices, institutional challenges, and contextual gaps at the National Bank of Ethiopia, which remain under-investigated in the local setting.

A qualitative approach, particularly content analysis, was deemed appropriate to capture the depth and complexity of stakeholder experiences, institutional dynamics, and practical implementation barriers that are often not measurable through purely quantitative methods. This method allows the researcher to derive meaning directly from participants' perspectives and institutional documents, thereby grounding the proposed framework in empirical realities rather than theoretical assumptions. Thus, the choice of a qualitative design is not due to a lack of existing literature in the broader field, but due to the need for a contextualized and interpretive understanding necessary to design a tailored ISRM framework suitable for the operational and regulatory environment of the National Bank of Ethiopia.

3.7. Validity and Reliability

3.7.1. Validity

Ensuring validity in qualitative research is essential to establish the trustworthiness and credibility of findings. In this study, content validity was achieved through expert review and theoretical alignment. The interview guide was developed based on established constructs from the Risk IT Framework, covering the domains of risk governance, risk evaluation, and risk response. The instrument was reviewed by professionals with expertise in IT risk management.

In order to reduce risks to the validity of this research, the researcher undertook several deliberate actions. To reduce researcher bias, the guidelines of Field and Morse (1985) were followed, recommending rigorous interviewer training prior to qualitative data collection. Accordingly, the researcher participated in multiple online and in-person trainings related to IT risk management, which facilitated the establishment of trust and rapport with participants.

Purposive sampling was employed to minimize sample bias by selecting participants with relevant knowledge of the research topic. The researcher exercised informed judgment to identify

individuals capable of providing rich and meaningful insights into information system risk management practices.

Additionally, the study's purpose and methodology were clearly communicated to participants. Two days prior to each interview, briefing sessions were conducted to explain the study's objectives, data collection procedures, and intended use of information. This approach fostered trust and improved data quality and authenticity. Overall, these steps ensured that the interview instrument adequately captured the breadth and depth of issues relevant to information system risk management at the National Bank of Ethiopia.

3.7.2. Reliability

Reliability in qualitative research pertains to the consistency and dependability of the research process and findings. Several strategies were applied to enhance reliability in this study:

Inter-coder reliability: A second independent reviewer cross-checked a sample of coded transcripts. Discrepancies were discussed and resolved through consensus, enhancing the objectivity of the analysis.

Audit trail: Detailed documentation of coding schemes, theme development, and interpretative decisions was maintained to ensure transparency and traceability.

Reflexivity: The researcher engaged in ongoing self-reflection to identify and mitigate potential biases, thereby maintaining fidelity to participants' perspectives.

3.8. Triangulation

To further enhance the credibility and confirmability of findings, methodological triangulation was employed. Data were collected from multiple sources including semi-structured interviews, organizational documents, and relevant literature to corroborate interpretations and minimize systematic bias.

3.9. Chapter Summary

This chapter presented the research design and methodology, clarifying that the study adopted a qualitative design with an inductive approach. The case study method was employed as the research strategy. Data collection instruments namely face-to-face interviews and document analysis were described as means to gather relevant and in-depth information. Measures taken to ensure validity and reliability were discussed. Finally, the data analysis process was outlined. The subsequent chapter will present the research findings, analyze the data, and discuss their implications.

CHAPTER FOUR
DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.1. INTRODUCTION

This chapter presents the findings obtained through interviews, document reviews, and inductive analysis. The data are introduced, analyzed, and discussed in relation to the research questions. The discussion establishes links between the research questions and the emergent themes. Findings from face-to-face interviews with representatives of the Information Systems Management Directorate (ISMD), the Internal Audit and Risk Management Directorate (IARM), and business unit participants are presented separately to reflect their distinct perspectives. Relevant internal documents were also reviewed to support triangulation and validate the primary data. While the data are organized by stakeholder group, the analysis and discussion are structured according to the three key domains of the Risk IT Framework: Risk Governance, Risk Evaluation, and Risk Response (ISACA, 2009). The analytical process follows an inductive approach, as described in Section 3.6, allowing themes and patterns to emerge naturally from the data without imposing predefined theoretical assumptions.

4.2. Respondent Information

The study respondents included IT staff, internal audit and risk management personnel, and business staff occupying managerial roles with significant responsibilities in information system risk management. Key job titles represented among the participants include ISMD Directors, Chief IT Security Officer, Chief Infrastructure Management Officer, Chief Database Administration Officer, Chief Application Management Officer, Chief IT Supervision Officer, Chief Risk Management Officer, Chief Payment Settlement Officer, Senior Currency Management Officers, and Chief Finance Management Officers.

4.3. Data Presentation

4.3.1. Data from Interview

4.3.1.1. Key IT Challenges in the Bank

To ensure anonymity while distinguishing between different stakeholder groups, participants are identified using codes such as P1–P6 (Information System Management Directorate), P7–P8 (Internal Audit and Risk Management), and P9–P11 (Business Units). The letter "P" denotes

"Participant," followed by a unique number for reference. When participants were asked about the most significant IT-related challenges facing the organization and how these issues impact daily operations, a number of recurring and interrelated themes emerged. These challenges reflect critical weaknesses in infrastructure, human capacity, governance, and operational processes.

A frequently mentioned challenge was the lack of adequately trained IT personnel. Multiple participants pointed out that the absence of regular and structured training programs limits staff capability to adapt to new technologies, detect vulnerabilities, or manage evolving systems. As P1 explained, "The absence of well-equipped talent and regular training makes it difficult to adopt or maintain new technologies. As a result, vulnerabilities are not easily identified." P6 also echoed this concern, stating that the lack of continuous training compromises the organization's ability to manage risk effectively.

Another dominant issue raised was the existence of outdated infrastructure and legacy systems. These systems were described as not only inefficient but also a major source of operational risk and cost. P1 mentioned that these legacy systems lead to "reduced efficiency, higher maintenance costs, and limited scalability." Similarly, P9 noted that the outdated infrastructure hinders the NBE ability to integrate new technologies and respond to change, causing delays and inefficiencies across departments.

Closely tied to these issues is the absence of a formal information system risk management structure. P2 and P7 noted that, the responsibility for information system risk management currently rests with the Internal Audit and Risk Management department, which lacks the technical expertise to handle information system specific risks effectively. This has led to key information system risks being either improperly assessed or overlooked entirely. The result is weakened risk mitigation and increased exposure to potential failures or cyber incidents.

P3 further highlighted a lack of foundational governance structures. The organization, they explained, does not have an officially approved information system risk strategy aligned with its mission and goals. Key guiding documents such as information system risk policies and procedures are either missing or not endorsed by the board. This vacuum in governance contributes to a broader lack of clarity in roles, responsibilities, and accountability. Tasks are

often performed based on individual initiative rather than standardized procedures, and important resources like IT inventory are not managed properly or kept up to date.

Operational challenges were also noted in day-to-day management and issue resolution. P4 observed that there is no structured incident tracking or problem management process in place. This results in repetitive issues going unresolved, as there is no formal mechanism to record, investigate, or learn from past problems. The lack of documented processes makes it difficult to analyze root causes or prevent recurrence. Altogether, the challenges identified by participants paint a picture of an IT environment burdened by outdated systems, untrained personnel, weak governance, and reactive operations. These issues not only disrupt normal functioning but also place the organization at considerable risk, particularly in an era where agility, resilience, and digital capability are essential for success.

4.3.1.2. Existing IT Risk Management Approach at NBE

Data were collected from two key stakeholder perspectives to ensure a comprehensive understanding of Information Systems Risk Management practices within the National Bank of Ethiopia. Participants are identified using the code "P" to denote 'Participant,' followed by a unique number for reference. The first group includes participants from the Information System Management Directorate and the Internal Audit and Risk Management Directorate (P1–P8), representing the technical and oversight functions. The second group comprises participants from Business Units (P9–P11), reflecting the operational and end-user perspective. This coding approach ensures both confidentiality and clarity in presenting qualitative findings.

Business Unit perspectives

When participants were asked about how information system risk is currently managed at the National Bank of Ethiopia, their responses pointed to a reactive and fragmented approach, with minimal integration between IT, business units, and the risk management function.

According to interviewees, the risk management department formally oversees IT risks, yet it lacks deep technical expertise. P9 explained that this limitation affects the department’s understanding of operational risks, particularly those emerging from fintech integrations and complex IT systems. Furthermore, operational units primarily play a passive role, submitting updates when requested rather than actively contributing to risk analysis or mitigation planning.

Participant was asked about the effectiveness of current risk management processes, and P10 described the approach as largely document-driven rather than proactive. Updates are submitted on an annual basis when formally requested; however, there is no ongoing, real-time feedback loop to monitor, report, or respond to emerging information system risks management. Consequently, this procedural framework fails to capture the dynamic and evolving nature of information system risk management. Similarly, P11 acknowledged that information system risk management awareness within their department is limited. Rather than actively engaging with IS risk management, business units often deferring these concerns to the IT team, with minimal communication unless the risk directly affects budget execution or financial reporting. This reflects a silos process, where business units remain disengaged from identifying or addressing information system-related risks unless the impact is immediate and operational.

4.3.1.3. Risk Governance

Establishing and Maintaining a Common Risk View
ISMD and Internal Audit Risk Management Department perspectives

Participant was asked about how a shared understanding of IT-related risks is established and maintained among various departments and stakeholders within the NBE. Their responses revealed significant concerns about the absence of an integrated IT risk governance structure and a lack of a clearly communicated risk view across the institution.

Participant was asked about the existence of a formal enterprise risk management (ERM) framework, and many expressed concerns over its absence. As P1 noted,

"…Our organization has not yet aligned its information system risk management activities due to the absence of an ERM framework and clearly defined roles."

This highlights the foundational gap preventing a unified risk perspective. Similarly,

P5 stated,

"…No formal information system risk management framework has been developed to reflect the bank overarching strategic objectives." As a result, critical aspects of information system risk management remain fragmented.

Participants were also asked about how IT risk appetite is formulated and integrated into operational processes. Responses indicate a disconnect between strategic risk formulation and practical implementation. As P2 explained, “An IS risk appetite draft has been defined by external consultants and is now overseen by IARM. However, the operational IT department (ISMD) is formal not involved in managing this risk appetite.” This further demonstrates that key stakeholders are excluded from risk-related decisions. Similarly, P6 reiterated, “Despite being directly impacted by IT risk decisions, ISMD is not involved in setting or managing risk appetite.” This exclusion weakens the bank ability to maintain a cohesive risk management approach.

Participant were asked about information system risk policies and how they align with institutional strategy. A shared concern among respondents was the absence of a structured policy linking IS risk management to the bank strategic direction.

P4 pointed out,

“…there is no IS risk policy or procedure that is aligned with the bank strategic objectives.”

This suggests that efforts to formalize risk governance remain inadequate. Similarly, P7 confirmed, “Currently, the bank lacks a defined IS risk policy or procedure that ties directly to its strategic goals.”

participants were also asked about the mechanisms in place at NBE to ensure a shared perception of IS risks between technical departments and business units. Their responses indicate that such mechanisms are either underdeveloped or entirely lacking.

Interviewees were asked about structured collaboration between ISMD and business units in managing IS-related risks. A common theme among responses was the lack of formal integration. P1 stated, “There is currently no well-organized approach to align the bank’s IS risks with business unit objectives through collaboration with the ISMD technical teams.” As a result, IS risk management efforts are not effectively integrated with the bank overall business strategy. Similarly, P4 emphasized, “There is no formal mechanism in place to ensure that ISMD and business units share a common understanding of risks.”

Participant were asked about the existence of an oversight body for IS risk governance, and many expressed concerns over its absence. P5 pointed out, “At present, NBE does not have a dedicated governance body or committee tasked with managing IS risk. While the IMF has advised forming a steering committee, their proposal centers on operational coordination rather than holistic IT risk governance.” This suggests that external recommendations focus on tactical collaboration rather than comprehensive oversight. P7 reinforced this concern, stating, “The bank lacks an established governance framework or committee specifically for information system risk oversight.” Similarly, P8 added, “Recommendations from the IMF include forming a coordination committee, but this does not address the full governance and strategic oversight required.”

Participant were asked to evaluate the integration of information system risk management within NBE broader risk governance framework, and their responses consistently reveal gaps in formal structures, governance mechanisms, and interdepartmental alignment. Addressing these deficiencies requires the establishment of a centralized ERM framework, improved coordination between technical and business units, and strategic policies that ensure IS risk management is embedded within the broader organizational risk strategy.

Business Units perspectives

When participant were asked about how the NBE defines and communicates its IS risk appetite and tolerance levels, their responses revealed significant gaps in tailored risk governance and oversight structures. According to participant, while a broad risk appetite exists, information system specific risk thresholds remain undefined, leading to a lack of clarity and alignment across departments. P9 pointed out that while risk management formally oversees IT risks, there is lack structured engagement between information system risk and strategic planning teams. As a result, operational units have limited input in discussions regarding systems that directly impact their work.

Similarly, P10 noted that risk tolerance regarding mission-critical systems, such as currency tracking tools, is not clearly communicated. These disconnect between the central risk framework and the actual risk perception at the operational level creates uncertainty in managing IT vulnerabilities effectively. Furthermore, P11 highlighted that budget allocations are not explicitly linked to IT risk appetite, leaving planners without clear prioritization of IT risk

management efforts. Without financial clarity, investment in risk mitigation measures becomes inconsistent, further worsening governance challenges.

Participant was also asked about governance structures responsible for overseeing information system risk. Their responses indicated that while the Internal Audit and Risk Management Directorate plays a formal role, there is no dedicated information system risk committee to ensure that technological risks are appropriately integrated into strategic decision-making. P9 emphasized that the absence of an information system specific governance body means that many business implications of information system risks go unaddressed.

Similarly, P10 noted that operational teams lack direct representation in risk-related governance, with most decisions being handed down from higher management levels with limited visibility for frontline units. This top-down approach, in turn, restricts proactive engagement and creates gaps in real-time risk communication. P11 also pointed out that financial planning is not well integrated into IT governance, leading to delays in risk-related budget allocations.

Integration with Enterprise Risk Management (ERM)

ISMD and Internal Audit Risk Management Department perspectives

Interviewees were asked about the existence of a formal ERM framework within the National Bank of Ethiopia, and the responses indicate that no such structure is currently in place. P4 emphasized, "Risk management practices are distributed, and there is no centralized ERM framework that includes IS risk as part of the broader enterprise risk profile." This suggests a fragmented approach where IS risk is not systematically embedded within enterprise-level risk strategies. In addition, Participant 7 noted, "The absence of an approved ERM framework results in IS risks being managed separately, which can lead to inconsistencies in risk prioritization." This further demonstrates that without structured integration, IS risks may not be effectively assessed alongside broader business risks, leading to misaligned responses.

Participant were asked about mechanisms ensuring alignment between IS risk management and business objectives. Many participants highlighted gaps in coordination that hinder effective risk governance. As Participant 1 observed, "There is currently no well-organized approach to align the bank IS risks with business unit objectives through collaboration with the ISMD technical teams. As a result, IS risks management efforts are not effectively integrated with the bank

overall business strategy." This underscores a disconnect between IS risk processes and enterprise-wide risk considerations. Similarly, P5 remarked, "Currently, mechanisms to align IS risks with business objectives are underdeveloped, leading to isolated risk management efforts." This suggests that IS risk management operates in silos rather than as part of a cohesive enterprise-wide system. P2 further explained, "The IARM department maintains an IS risk register and coordinates with ISMD, but formal alignment mechanisms between IT and business units are limited. He said

" … while some level of coordination exists, it lacks the structured approach necessary for comprehensive risk integration.

Participant was asked about the consistency of risk perception among technical teams. Several responses indicate that risk understanding is fragmented not only between ISMD and business units but also within ISMD itself. P3 provided a critical internal observation, stating, "there is not a common perception, even within technical teams." This suggests discrepancies in how IT teams interpret and manage risks, further complicating alignment efforts. Similarly, P8 noted, "There's a lack of organized collaboration between IT and business units, resulting in misaligned risk perceptions and strategies." This reinforces the necessity of structured integration mechanisms.

Participant was asked about existing risk management practices within specific departments. Some coordination was identified, but it remains operational rather than strategic. P6 said,

"…It is under IARM department where that risk team sets the IS risk register and discusses with the ISMD concerning IT."

While this interaction indicates some operational-level coordination, it does not reflect full ERM integration. Furthermore, P7 explained, "lack of integrated risk management processes means that technical and business teams often operate with differing risk priorities." This demonstrates that without centralized oversight, IS risk responses lack coherence at the institutional level.

Business unit Perspectives

When Participants were asked about how IS risk is integrated into the broader Enterprise Risk Management (ERM) framework at the NBE, their responses pointed to a fragmented and

informal approach, primarily due to the absence of the ERM framework. According to Participants, IS risk is currently handled in isolation, without structured alignment with enterprise-wide priorities. P9 noted that the ERM framework remains in draft form and has yet to receive formal approval from management. As a result, IS risk management is confined to the Internal Audit and Risk Management team, with no defined mechanism for mapping IS-related risks to broader organizational concerns. Furthermore, business units have limited involvement in IS risk discussions, leading to a silos approach to risk identification and mitigation.

Participants were asked about the current handling of IS risk documentation, and P10 explained that while IS-related issues are recorded manually, their integration into the general operational risk reports is informal. Consequently, without a structured ERM framework, IS risks are not systematically addressed in alignment with enterprise-wide objectives. This lack of integration, in turn, weakens the ability of the organization to anticipate, assess, and manage IS-related vulnerabilities effectively.

Additionally, P11 highlighted that IS risk does not have clear visibility from a budget perspective. Rather than being seen as a strategic priority, IS risks are often treated as a cost burden. As a result, financial allocations for IS risk mitigation remain inconsistent, hindering the organization's ability to proactively manage IT security, compliance, and operational resilience.

Making Risk-Aware Business Decisions

ISMD and Internal Audit Risk Management Department perspectives

Participants were asked how the NBE utilizes information system risk information to guide critical business decisions, such as investments in digital payment systems or vendor selection, and what processes support this integration. Their responses suggest that IS risk considerations are not systematically embedded into the bank’s strategic or operational decision-making processes.

A key concern among participants is the lack of structured reporting that ensures IS risk data informs high-level business decisions. As P1 remarked, “the risk department does not provide concrete or structured reports to senior leadership to support decisions on upgrading systems and infrastructure.” As a result, IS risk insights do not directly shape major technology investments. Similarly, P5 stressed, “Without timely and accurate IT risk information, decisions regarding

digital investments are made with limited risk insight." This further demonstrates that risk awareness is not consistently incorporated into investment strategies.

Participants were asked about the factors influencing IS-related business choices. Responses indicate that compliance mandates exceed internally driven risk evaluations. P2 explained, "Cyber security risk identification and assessment are led by the IT Security team with support from INSA. Business decisions are shaped more by compliance requirements than by internally driven IT risk evaluations." This suggests that IS risk considerations are reactive rather than proactively embedded in decision-making.

In addition, P6 shared, "Before launching any digital financial operations, institutions are required to obtain a license from INSA, ensuring they meet mandatory IT security requirements. Thus, information system risk information is used mainly in compliance with external mandates rather than through internal business-aligned evaluation mechanisms." This further highlights that risk assessment is framed as a regulatory obligation rather than a strategic business tool.

Several Participants pointed out the lack of structured processes that explicitly connect IS risk assessments with business strategy. P3 observed,

"…there is no integrated risk decision framework that explicitly connects IS risk with strategic business decisions. Additionally, the bank relies on general guidelines and past experiences."

Without a structured approach, risk assessments may not consistently impact investment or technology-related decisions. Similarly, P7 added, "The current processes do not effectively incorporate IS risk assessments into decision-making for new technologies or partnerships." This indicates that I risk considerations are disconnected from innovation and vendor-related decisions.

Participants were asked to describe instances where IS risk awareness had a tangible impact on business decisions at NBE. Their responses suggest that limited cross-functional communication and inconsistent risk awareness hinder IS risk from meaningfully influencing business strategies. A recurring concern among Participants is the lack of collaboration between departments, leading to outdated risk perceptions. Participant 1 noted, "The concerned department has not provided sufficient awareness or training on IT-related risks to bank employees. Additionally,

there are systems that have already been upgraded by the bank, yet the risk register maintained by the risk department still references outdated versions." This illustrates a disconnect between IT risk updates and organizational decision-making. Similarly, Participant 5 reinforced this challenge, stating, "The lack of cross-functional communication has resulted in outdated risk registers, which fail to reflect current system statuses." As a result, decisions may be made based on incomplete or outdated risk data.

In addition, interviewees were asked about internal IT risk awareness initiatives. Participant 3 provided a comparative perspective, explaining, "There is an IT risk management directive for all commercial banks licensed in Ethiopia, but internally, the same level of risk awareness does not exist." This suggests that while external banks follow structured risk guidelines, NBE lacks equivalent internal practices. Participant 7 emphasized the consequences of low awareness, stating, "Due to insufficient awareness of IT risks, some business decisions have not adequately accounted for potential vulnerabilities." This further demonstrates that risk awareness must be strengthened for better decision-making.

Despite these concerns, some initiatives do exist to enhance awareness. Participant 4 stated, "The security team regularly publishes awareness materials such as printed booklets, internal notifications, and Outlook pop-up messages about ongoing cyber security threats and best practices." While these efforts help individual awareness, they do not necessarily inform high-level strategic business decisions. Similarly, Participant 6 shared, "Through the IT risk register, we are daily aware of areas of risk." However, the effectiveness of this practice in influencing broader business decisions remains unclear.

Business Unit Perspectives

When Participants were asked about how the National Bank of Ethiopia incorporates IT risk intelligence into business decision-making particularly in areas such as digital payment systems and vendor partnerships their responses revealed gaps in structured risk-based evaluation. According to interviewees, IT risk considerations do not play a central role in guiding major business decisions. P9 noted that while investments in vendor partnerships and new payment platforms occur, business units responsible for managing IT risks are rarely consulted. Without a formalized risk-based decision framework, IT-related vulnerabilities remain unaddressed until after implementation, increasing operational uncertainty.

Participants were asked about how system upgrades are handled in relation to risk evaluation. P10 explained that these decisions are typically made at the central level, with operational teams often informed only after implementation. Consequently, this lack of preemptive consultation means that potential IT risks including security vulnerabilities and infrastructure compatibility may not be adequately assessed before deployment. Additionally, P11 emphasized that IT risks are only prioritized when they carry major financial implications. Rather than maintaining a structured process for risk-driven investment strategies, budget allocations tend to react to immediate financial pressures rather than proactive risk intelligence. This approach, in turn, limits the institution's ability to mitigate long-term technological risks and align IT investments with a broader enterprise strategy.

4.3.1.4. Risk Evaluations

Collect Data

ISMD and Internal Audit Risk management Department perspectives

Participants were asked how the National Bank of Ethiopia collects and manages data on IS risks, including incidents, vulnerabilities, and threats. Their responses reveal a fragmented, largely manual approach characterized by limited integration, inconsistent formats, and a reactive reporting culture. A prevailing concern among participants is the lack of a centralized system for IS risk data collection. As Participant 2 noted, "IS risk data is recorded in separate registers across departments, leading to data silos, inconsistent formats, and limited visibility across the organization." This further demonstrates that risk data management remains disjointed, making it difficult to develop a cohesive enterprise-wide IS risk profile. Similarly, Participant 6 elaborated, "Rather than maintaining a centralized risk register, NBE manages IS risk data through multiple, department-level registers. These fragmented records include risk information handled by different teams but are not integrated into a single, unified system." As a result, risk assessment and mitigation efforts lack coordination and visibility across the organization. In addition, P4 observed, "There is no formal risk register, and potential threats are not consistently logged or tracked. Additionally, the bank does not have a centralized system for monitoring and managing risk-related data." This highlights a critical weakness in proactive risk identification.

Another recurring theme among responses is the reliance on periodic updates rather than real-time risk tracking. As P1 explained, “The risk department sends to business units to update the risk registry annually.” While structured, this process does not support continuous risk monitoring and may result in outdated information. In addition, P7 confirmed this challenge, stating, “The current approach to managing IS risk data is reactive, relying on annual updates rather than continuous monitoring.” This suggests that emerging risks may not be captured in a timely manner.

Similarly, P5 reinforced the concern, remarking, “Data on IS risks is primarily gathered through periodic reports, which may not capture emerging threats promptly.” As a result, risk mitigation efforts may be delayed. P8 reiterated this issue, stating, “The risk department requests annual updates to the risk register from business units, but this process lacks real-time data collection.” This further demonstrates that existing methods do not sufficiently support proactive risk evaluation.

Despite these challenges, some participants acknowledged that certain IT security teams have mechanisms for data collection. P3 noted, “There are tools in the security teams that collect logs and communicate with INSA.” While this indicates some level of operational data collection, the lack of integration into broader risk reporting limits its effectiveness.

Participants were asked to identify who is responsible for gathering and validating IS risk data at NBE and how frequently this data is updated. Their responses suggest shared responsibility between the Internal Audit and Risk Management Directorate (IARMD) and senior IT leadership, but with limited coordination and infrequent updates. Most participants consistently identified the IARMD as the main body responsible for IS risk data collection. P1 stated, “Internal Audit and Risk Management Directorate (IARMD).” This is echoed by P2, who confirmed, “The IARM department is responsible for collecting and validating IT risk data.” Similarly, P4 added, “Internal Audit and Risk Management departments facilitate the collection and validation process.” While this suggests a shared function, it may lack a central focal point for ensuring consistent and frequent updates.

One of the most common concerns raised by participants is the infrequency of data updates. As P5 pointed out, “Responsibility lies with the Internal Audit and Risk Management Directorate,

but the infrequent updates may not reflect the current risk landscape." This raises concerns about the effectiveness of IS risk assessments in a rapidly evolving digital environment. In addition, P7 reinforced this challenge, explaining, "The Internal Audit and Risk Management Directorate manages IS risk data, but the lack of frequent updates can hinder timely risk mitigation."

Beyond IARMD, Participants identified senior leadership as key stakeholders in interpreting IS risk data for strategic decision-making. As P8 explained, "Responsibility for reviewing the IS risk profile lies with ISMD directors and top management, who use the information to guide decision-making processes at the governance level." This suggests that while collection and validation may be handled by IARMD, interpretation and strategic application involve executive leadership.

Risk Analysis

ISMD and Internal Audit Risk management Department perspectives

Participants were asked to describe the methods, tools, and techniques used at the National Bank of Ethiopia to assess the likelihood and impact of IS risks, including those related to digital payment systems and data breaches. Their responses indicate that while some basic classification approaches exist, the current methods lack sophistication and fail to fully address the evolving IS risk landscape.

Participant's consistently highlighted concerns regarding the simplicity of NBE IS risk classification. As P1 explained, "The risk department uses a simple categorization approach in the risk register, classifying risks as 'high, medium, and low.' However, these classifications are not aligned with the current IS risk landscape, particularly as new technologies and threats have evolved." This suggests that outdated classifications may underestimate or overlook significant IS risks. Similarly, P8 reiterated, "Risk assessments are categorized as high, medium, or low, but these classifications may not align with the complexities of modern IT threats." As a result, emerging vulnerabilities may not be properly accounted for.

In addition, Participants were asked about the specific techniques used to assess IS risk probability and impact. P2 noted, "Risk registers contain labels for probability, impact, and risk scores, but assessments are conducted by personnel who lack specialized IT risk expertise." This further demonstrates the need for improved technical knowledge in risk evaluation. P6 confirmed

this approach, stating, “NBE uses risk registers that incorporate labels for probability, impact, and risk scores to assess the likelihood and impact of IS risks, including cyber threats and data breaches, but experts lack knowledge.” This indicates that while basic frameworks exist, they may not be effectively applied.

A commonly expressed concern among participants is the inadequacy of current tools in assessing risks associated with evolving technologies. P5 observed, “The current tools lack the granularity needed to effectively assess risks associated with emerging technologies.” This suggests that existing risk assessment mechanisms do not provide sufficient detail or adaptability. Similarly, P7 stressed, “Our assessment techniques need to evolve to accurately capture the likelihood and impact of sophisticated IS risks.” This further demonstrates the need for updated evaluation frameworks that address complex digital threats.

Interestingly, P4 described a specific technical security measure rather than a formal risk assessment methodology: “We rely on hardware tokens and electronic tokens as part of our multi-factor authentication process, which ensures secure access to critical systems.” While this highlights a security control, it does not represent a systematic approach to risk analysis.

Participants were asked how NBE evaluates emerging IS risks and integrates them into decision-making processes. Their responses reveal a mixed approach, with some external collaboration but significant gaps in systematically addressing new threats.

Several participants noted partnerships with outside institutions for identifying risks. As P2 explained, “The IT Security team collaborates with the Information Network Security Administration (INSA) to identify emerging risks. This process involves analyzing audit findings, reports, and industry trends, particularly around digital payment systems and vendor vulnerabilities.” This suggests that external assessments contribute to risk identification.

Similarly, P6 added, “The IT Security team, in partnership with INSA, collects data from audits, security reports, and industry trends, focusing on high-risk areas such as data breaches in digital payment systems and vulnerabilities in vendor partnerships.” While external engagement provides valuable insights, a structured internal framework is still necessary. In addition, P4 mentioned, “Consultants are formed at NBE to assess new technology trends, particularly in the

realm of digitalization, with the aim of integrating these trends into the bank's IT risk analysis." This further demonstrates that advisory efforts exist but may not be fully institutionalized.

Despite these efforts, several participants expressed concerns about weaknesses in how emerging IS risks are incorporated into strategic decision-making. P5 observed, "The integration of emerging risks into our analysis is limited, potentially leaving us vulnerable to new threats." This suggests that despite some external collaboration, internal mechanisms remain insufficient. Similarly, P7 stressed the need for improvement: "Our decision-making processes need to better incorporate assessments of emerging IS risks to stay ahead of potential issues." This highlights the urgency of refining risk evaluation strategies to proactively mitigate threats. P8 summarized the concern, stating, "our risk assessment methods are not fully aligned with the current technological landscape."

Business Units Perspectives

When interviewees were asked about how the National Bank of Ethiopia evaluates and integrates emerging technology risks into its Information system risk analysis and decision-making processes, their responses indicated a lack of structured monitoring and proactive risk incorporation. According to Participants, the bank does not have a formalized mechanism to systematically track or assess new IS risks within its broader risk management framework. P9 explained that emerging risks are not evaluated through a structured process, meaning there is no clear method for escalating, integrating, or addressing technological threats in alignment with enterprise-wide risk management. Without a dedicated system, IS risk identification remains fragmented, leaving the institution vulnerable to unforeseen disruptions.

Participants were asked about the communication of IS risk intelligence across departments. P10 noted that business units rely heavily on the ISMD department to assess and relay potential threats, but this approach has weaknesses. Since IS-specific risks are not always translated into operational contexts, decision-makers may fail to recognize their impact on business objectives. This lack of structured communication, in turn, leads to gaps in risk prioritization and preparedness. Additionally, P11 highlighted misalignments between budget planning and emerging risk intelligence. IS risks are rarely incorporated into financial planning unless explicitly raised by the IS department. Rather than proactively allocating resources for risk

mitigation, financial decisions often focus on immediate needs, neglecting long-term resilience strategies. This misalignment weakens the bank's ability to anticipate and invest in protective measures before risks materialize.

Maintaining Risk Profile

ISMD and Internal Audit Risk management Department perspectives

Participants were asked how the National Bank of Ethiopia maintains and updates its IT risk profile to keep pace with evolving threats, particularly those emerging from Ethiopia's expanding fintech ecosystem and global cyber security trends. Their responses consistently highlight challenges related to outdated risk management practices, compliance driven oversight, and the absence of real-time threat monitoring.

A key concern among participants is that NBE IS risk profile does not adequately reflect the rapidly evolving digital finance landscape.

As Participant 1 said,

"…We are currently lagging behind the global financial sector in terms of updating and maintaining our IS risk profile."

This delay increases exposure to emerging cyber threats and compliance risks, placing the bank at a competitive disadvantage. Similarly, P8 summarized this concern, stating, "Our current IS risk profile does not adequately reflect the rapid developments in fintech and global cyber security." As a result, the institution remains vulnerable to evolving risks.

In addition, several participants emphasized that IS risk profiling at NBE is primarily influenced by external regulatory enforcement. Participants 2 and 6 noted, "The IS risk profile is governed by a cyber-security policy and subject to external enforcement by INSA, which requires mandatory clearance before launching any new system or product." This further demonstrates that risk assessments are largely compliance-driven rather than strategically integrated.

Participants also highlighted the need for a structured, proactive approach to IS risk profiling. P5 pointed out that "the risk profile is not dynamically updated." While some emerging risks are captured through "periodic audits or incident reports," the bank lacks a "structured framework or

ongoing threat intelligence process." As a result, the institution struggles to monitor innovations in fintech and evolving cyber threats effectively. Similarly, P7 described the risk profile as "largely static and lacking real-time threat monitoring." Given the rapid growth in digital finance and increased connectivity to international systems, they stressed a "pressing need to enhance threat modeling capabilities and adopt continuous risk assessment practices." This further demonstrates the necessity of integrating real-time risk monitoring mechanisms.

Participants were asked about the key actors responsible for reviewing and utilizing NBE IS risk profile. Their responses indicate that responsibility is primarily shared between the Internal Audit and Risk Management Directorate (IARMD), senior management, and ISMD leadership. Several participants consistently identified IARMD as a central body in IS risk profile management. Participants 1, 4, and 5 confirmed, "The Internal Audit and Risk Management departments are key actors responsible for reviewing the IS risk profile and facilitating the collection and validation of IS risk data." This ensures a formalized structure for risk review, though its effectiveness depends on update frequency. However, P5 noted a critical limitation: "Infrequent updates to the risk profile may undermine its relevance to the current risk landscape." This suggests that despite oversight by risk management teams, the profile lacks timely revisions.

In addition, Participants were asked about how IS risk insights are utilized at the governance level. P2, P 6, P 7, and P 8 emphasized that senior management and ISMD play a significant role in reviewing the IS risk profile. They use information from risk registers to inform mitigation actions and guide strategic decision-making processes. As P8 explained, "Risk profiling at the governance level ensures that leadership remains informed about critical IS risks and incorporates this insight into high-level business decisions." This demonstrates the importance of executive engagement in IT risk strategy.

Business Units Perspectives

When Participants were asked about how the National Bank of Ethiopia ensures it's IS/IT risk profile remains updated to reflect evolving threats such as those arising from Ethiopia's expanding fintech ecosystem and global cyber security trends their responses pointed to a lack of structured risk monitoring and adaptation. According to Participants, the bank does not have a centralized or regularly updated IS risk profile, making it difficult to align risk identification with

technological advancements and emerging threats. P9 noted that while the fintech ecosystem continues to evolve, internal policies and systems are not keeping pace, creating inconsistencies in risk exposure. Without active engagement, departments responsible for IS risk management remain disconnected from industry shifts, reducing the bank's ability to anticipate vulnerabilities effectively.

Participants were asked about existing frameworks for tracking and integrating IS risks. P10 explained that individual departments may document specific risk factors informally, but no structured mechanism exists to continuously assess and reflect changes in the broader threat landscape. Consequently, the absence of a coordinated risk review process limits the ability to conduct proactive planning and strategic risk mitigation. Additionally, P11 emphasized that IS risk identification remains fragmented across departments. Rather than maintaining a structured and systematic process for assessing new risks, the bank’s approach tends to be reactive. These misalignment, weaken comprehensive risk governance and reduces responsiveness to emerging fintech challenges and cyber security developments.

4.3.1.5. Risk Response

Articulating IT Risks

ISMD and Internal Audit Risk management Department perspectives

Participants were asked about how IS/IT risks, including cyber security threats and system failures, are communicated at the National Bank of Ethiopia. Their responses indicate that while external collaborations exist, internal communication processes lack formalization, consistency, and accessibility for non-technical stakeholder.

Participants were asked about NBE engagement with external institutions in IS risk communication. Several participants highlighted the Bank’s active collaboration with the Information Network Security Administration (INSA) and sector-wide forums for sharing cyber threat intelligence. As P1 noted, “We maintain direct communication with INSA and actively participate in a financial sector platform dedicated to sharing cyber threat intelligence.” This demonstrates inter-organizational cooperation that strengthens sector-wide resilience. Similarly, P2 explained, “Cyber security risks are managed through external enforcement by INSA, which

requires mandatory clearance before launching any new system or product." While this ensures compliance, it does not necessarily support a proactive internal risk response strategy.

Participants were asked about how IS risks are shared internally within NBE. Their responses indicate a lack of structured communication strategies. As P6 observed, "IS risks are communicated to non-technical persons within the bank. However, there is no indication of structured communication strategies or tailored reporting." This suggests that while risks are shared, the absence of standardized messaging limits their effectiveness. Similarly, P2 noted, "While IS risks are shared with non-technical staff, there are no structured communication strategies or templates in place to ensure clarity, especially for executive audiences." As a result, key stakeholders may not receive timely or comprehensible information.

Participants were asked about the methods used for reporting IS risk incidents. Many described a lack of standardization and coordination, resulting in delays in response. P5 explained, "There is no standardized communication protocol. Identification and communication of such events involve a trial-and-error process that delays responses." This further demonstrates inefficiencies in incident escalation. Similarly, P8 stated, "We rely on ad-hoc methods such as distributing printed warnings and broadcasting alerts through domain-joined systems. However, due to the lack of a structured incident response communication strategy, delays in understanding and responding to incidents are common." This highlights the need for a formal framework to improve incident reporting.

Participants were asked about how IS risks are communicated to non-technical staff and decision-makers. Many responses indicate challenges in translating technical risks into accessible language. P1 stated, "The level of communication is very low." This highlights a fundamental weakness in ensuring IS risk information is understandable and actionable. Similarly, P3 noted, "IS risks are not communicated effectively to non-technical stakeholders." This suggests a systemic gap in risk messaging and cross-functional understanding.

Participants were asked about training programs supporting IS risk awareness. Their responses consistently indicate that a lack of structured education further complicates communication challenges. As P4 explained, "There is a lack of continuous training, which makes it difficult for non-technical stakeholders to fully understand and respond to IS risks." This demonstrates that

weak communication practices are compounded by inadequate educational efforts. Similarly, P5 reinforced this concern, stating, “Due to the absence of regular and targeted training, many non-technical staff struggles to understand the significance of IS risks or how to respond.” This suggests the need for structured awareness initiatives.

P7 added, “The bank does not yet have an effective strategy for translating technical IS risk information into language that non-technical managers or users can grasp. This often results in misunderstanding and underestimation of critical threats.” This further demonstrates the need for simplified communication methods.

Participants were asked about how IS risk information reaches executive leadership. While senior management is involved, responses indicate that the process lacks systematization. P4 explained, “The review of the IS risk profile is carried out by ISMD directors and senior management to ensure informed decisions at the governance level.” However, this engagement remains ad hoc rather than structured. Similarly, P8 noted, “Non-technical stakeholders are often not fully engaged or capable of acting on IS risk notifications because communications are either too technical or not delivered consistently.” This reinforces the need for structured, audience-specific risk communication strategies.

When Participants were asked about how the National Bank of Ethiopia communicates identified IS risks such as cyber security threats or system failures to decision-makers and relevant stakeholders, their responses pointed to a lack of structured, proactive engagement and risk-based reporting. According to Participants, IS risk communication typically occurs after an issue has already materialized rather than through a systematic early warning process. P9 explained that notifications are often sent via email or informal briefings from the IS team, but there is no structured framework to ensure clarity and timely risk dissemination. As a result, business units struggle to assess the financial and operational implications of IS threats. Without tailored communication, technical risks remain disconnected from business priorities, making it difficult for decision-makers to advocate for necessary mitigation measures.

Participants were asked about the effectiveness of information sharing mechanisms. P10 noted that communication is mostly incident-driven, with little structured information-sharing about vulnerabilities unless they directly impact specific teams. This reactive approach, in turn, limits

proactive risk awareness and preparedness across departments. Additionally, P11 highlighted that IS risk communication is ineffective from a financial perspective. Risks are rarely quantified in terms of financial exposure, making it difficult to integrate IS-related vulnerabilities into investment and budgetary planning. Without clear financial metrics, decision-makers may fail to recognize the urgency of IS risks or allocate sufficient resources to mitigate threats before they escalate.

When Participants were asked about how effectively IS risks are conveyed in terms that non-technical stakeholders can understand and respond to, their responses highlighted a lack of clarity, structured communication, and business-contextualized reporting. According to Participants, IS risk communication tends to be reactive rather than proactive, often occurring after incidents rather than through systematic early warnings. P9 emphasized that critical vulnerabilities are primarily communicated through incident reports rather than predictive alerts, leaving decision-makers in a position where they are responding to problems rather than anticipating them. Without forward-looking risk assessments, business units struggle to prepare for threats effectively.

Participants were asked about the accessibility of IS risk communication for non-technical stakeholders. P10 noted that IS-related threats are frequently described using technical language, making it challenging for departments outside of ISMD to grasp their severity or implications. This lack of contextualization, in turn, hinders informed decision-making and slows organizational responses to emerging threats. Additionally, P11 highlighted that while some warnings or alerts are shared, they lack actionable details especially in terms of financial exposure or operational impact. Without structured communication, business units may not fully understand how IT risks affect their strategic goals, making it difficult to prioritize mitigation measures.

Managing Risks

ISMD and Internal Audit Risk management Department perspectives

Participants were asked about how IT risks, including cyber security threats and operational vulnerabilities, are managed at the National Bank of Ethiopia. Their responses indicate that the Bank primarily relies on risk mitigation and risk acceptance strategies, with little evidence of

formal risk transfer mechanisms such as cyber insurance or outsourcing with defined risk clauses.

Participants were asked about the dominant approach to handling IS risks at NBE. Most participants cited risk mitigation through technical controls and policy enforcement as the primary strategy. As a result, the Bank prioritizes protective measures to address risks. P2 noted, "Mitigation is the primary strategy, using security tools and internal policies." Similarly, P6 explained, "The primary strategy for handling IS risks at NBE is mitigation, achieved through the deployment of security tools and enforcement of internal policy documents." In addition, P5 emphasized, "The Bank generally leans toward mitigation strategies, especially by engaging vendors or internal IS staff to contain incidents." This further demonstrates that both internal resources and third-party support play a role in controlling risks.

Despite a strong emphasis on risk mitigation, Participants consistently highlighted that these efforts tend to be reactive rather than proactive. As P1 observed, "Mitigation is pursued particularly for well-known or previously experienced risks by implementing basic controls, system patches, or upgrades. However, these efforts are often reactive rather than part of a structured risk management process." This suggests that risk response is event-driven rather than strategically planned.

Participants were asked about alternative strategies used when mitigation is not feasible. Risk acceptance emerged as a common response, particularly for emerging or low-impact threats. P1 explained, "Risk acceptance appears to be the most commonly applied IS risk response strategy, often due to limited resources, lack of timely communication between departments, or insufficient technical expertise within the risk function." As a result, certain risks are tolerated due to practical constraints. Similarly, P8 noted, "Occasionally, risks are accepted, particularly if they're seen as low impact or when mitigation requires resources beyond current capacity." This further demonstrates that financial and operational limitations influence risk acceptance.

Participants were asked about whether NBE employs risk transfer mechanisms such as cyber insurance or outsourcing with structured risk agreements. Their responses indicate that these approaches are largely absent. P6 explicitly stated, "There is no indication of formal use of risk transfer (e.g., cyber insurance) or structured risk acceptance processes with documented

tolerances or residual risk evaluation." This reinforces the Bank's reliance on internal risk handling rather than external coverage.

Participants were asked about structured response frameworks for IS risk incidents. Several participants raised concerns about the absence of formalized procedures, which weakens the consistency and efficiency of risk response efforts. P3 remarked, "There is an absence of a corporate communication strategy, incident response management plan, and crisis management strategy. The risk response is dependent on the type of risk that occurs and is based on identifying the impact of the risk." Similarly, P7 reinforced this, stating, "The absence of structured crisis and communication strategies makes long-term responses reactive rather than proactive." As a result, IS/IT risk incidents are handled inconsistently.

Participants were asked about decision-making authority for significant IS risks at NBE. Their responses indicate that final decision-making resides primarily with the executive leadership, specifically the Governor and Vice Governor, while operational insights are provided by functional teams such as ISMD and Risk Management.

Participants were asked about who holds the highest level of authority in IS risk decision-making. A majority of participants emphasized that senior management plays a central role in reviewing and responding to high-impact IS risks. P2 stated, "Decisions are primarily made by senior management, and in critical cases, escalated to the Board of Directors, depending on the nature and impact of the risk." Similarly, P6 explained, "The responsibility for making decisions related to significant IT risks lies primarily with senior management." This further demonstrates that executive oversight is key to risk response.

Participants were asked about specific individuals involved in IS risk decisions. Multiple respondents identified the Governor and Vice Governor as the final authorities responsible for IS risk management. P3 highlighted, "Top management, including the Governor and Vice Governor, are involved." This confirms that critical IS risks are managed at the highest leadership level. Similarly, P5 noted, "Decision-making authority lies with senior management, particularly the Vice Governor and Governor, to ensure alignment with strategic goals." Similarly, P4 reinforced this point, stating, "Decisions are made at the Vice Governor and

Governor levels, ensuring that the highest levels of leadership are engaged in risk management." As a result, IT risk decisions remain centralized.

Participants were asked about how operational teams contribute to risk-related decision-making. While final authority rests with executive leadership, functional teams provide key operational insights. P1 explained, "The Risk Management Team and ISMD are involved in the process." This suggests that technical expertise plays a supporting role in decision-making. Similarly, P8 clarified, "senior leadership, particularly the Governor and Vice Governor, are central to managing significant IS risks, but operational teams provide essential input to inform those decisions." And also P7 summarized the governance model concisely, stating, "Significant IS risk issues are escalated to executive leadership. The Governor and Vice Governor typically review such issues before any major decision or response strategy is adopted." This demonstrates a structured escalation process for managing critical IS risks.

Business unit's perspectives

When Participants were asked about who is involved in managing significant IS risks within the National Bank of Ethiopia, their responses highlighted a senior management-driven approach, with limited engagement from broader business units and a lack of structured risk governance. According to Participants, major IS risk decisions are primarily handled by senior executives, including Vice Governors and Directors. P9 noted that while the Risk Management Directorate plays a role in escalating IS-related risks to leadership, there is no dedicated IS risk committee to systematically assess and address these risks. As a result, decision-making tends to be reactive, often occurring only after risks have been flagged through audits or operational reports. This lack of centralized IS risk governance, in turn, creates gaps in aligning IT risk management with strategic priorities.

Participants were asked about the involvement of different teams in IS risk management. P10 explained that only IS and risk units actively participate in decision-making, while other departments play a passive role. Rather than contributing to discussions, business units typically receive risk-related updates without direct input in shaping mitigation strategies. This limited engagement restricts cross-functional collaboration and reduces the effectiveness of proactive risk management. Additionally, P11 pointed out that IS-related budgeting and responses are largely reactive. Without structured risk-based financial planning, IT security and infrastructure

investments often lack prioritization, making it difficult to address risks systematically. Furthermore, key business stakeholders are not consistently involved in early decision-making stages, further limiting strategic risk alignment.

React to risk Events

ISMD and Internal Audit Risk management Department perspectives

Participants were asked to describe how the National Bank of Ethiopia responds to IS incidents such as cyber-attacks or critical system failures. Their responses suggest a largely reactive and event-driven approach, with varying degrees of formality and coordination across departments.

Participants were asked about the initial steps taken when an IS incident occurs. A common theme among responses was the focus on containment and isolation of affected systems to prevent further damage. P5 stated, “We isolate affected systems by disconnecting external ports or lines to contain the issue.” Similarly, P7 noted, “We typically begin by disconnecting potentially compromised systems.” In addition, P8 elaborated that containment is often achieved by “severing network access points, followed by investigation led by a temporary task force.” These responses demonstrate that the Bank prioritizes quick isolation as a first-line defense against IS disruptions.

Participants were asked about how IS incidents are coordinated across departments. Several participants emphasized the formation of ad hoc response teams. P3 explained, “A task force is prepared from relevant departments to investigate the events or accidents.” Similarly, P7 added, “A cross-functional team is assembled to investigate,” with technical support from the Information Network Security Administration (INSA). This further demonstrates that while response teams are formed, they operate on an ad hoc basis rather than under a pre-established framework.

Participants were asked about external collaboration during IS incidents. Many responses highlighted coordination with INSA as a crucial part of the response process. P1 shared, “The organization communicates with the National Cyber Emergency Response Team to report and coordinate response efforts.” This was reinforced by Participant 5, who noted, “INSA is engaged depending on the severity of the incident,” and P8, who stated, “Coordination with INSA is

crucial in managing cyber-attacks or advanced threats." As a result, the Bank relies heavily on external support for cyber threat management.

Participants were asked about how NBE restores operations following major disruptions. While containment and investigation are emphasized, structured recovery approaches are deployed in specific cases. P1 explained, "For critical system failures affecting production environments, the organization initiates the Disaster Recovery (DR) process, which continues until production systems are fully restored, often with assistance from system vendors." Similarly, P2 noted, "The Bank uses critical tools to manage and mitigate known IS incidents and risks, while it tends to accept newer, less familiar incidents due to a lack of predefined response strategies." These responses indicate that while structured recovery processes exist for major disruptions, newer threats may be met with less clarity.

Participants were asked about major IS incidents that required reactive responses over the past year. Their responses revealed two key incidents: a critical storage system failure and a fire outbreak at the Disaster Recovery (DR) site.

One participant described an incident involving outdated storage devices, which disrupted the functioning of key systems by preventing data communication between core components. The Bank responded by activating its DR system, enabling temporary service continuation. With assistance from internal IT staff and system vendors, operations were eventually restored.

The participant identified several improvement areas, including:

Proactive infrastructure modernization

Asset lifecycle management

Preventive maintenance and monitoring

Strengthened DR testing and readiness

Improved IT risk communication

The second and more widely cited incident involved a fire at the DR site, located in Building #3. This event was mentioned by multiple participants. P3 stated, "The fire caused immediate

disruption to some IT infrastructure," adding that the "data center was partially affected, resulting in service outages." Similarly, P4 noted, "Improper power leakage, wrong installations, and the use of under-standard cables led to a fire that burned out a section of the DR site."

Despite the severity, the Bank's technical teams responded quickly. P2 remarked, "The response from technical teams was effective, which helped minimize downtime." However, the incident exposed vulnerabilities in physical infrastructure standards, cabling practices, and preventive maintenance routines. P7 commented, "The event exposed flaws in our physical infrastructure management." Similarly, P8 added, "It revealed a lack of preventive maintenance and infrastructure quality assurance." P5 summarized the lessons learned from the fire, stating, "While emergency response was swift, the incident highlighted the need for better infrastructure standards and proactive facility audits." These insights reinforce the importance of strengthening preventive measures to avoid future disruptions.

4.3.2. Document Review

As part of this study, a comprehensive document review was conducted to supplement primary data collected through interviews and to provide contextual insights into the National Bank of Ethiopia existing IT risk management. The reviewed materials included internal policies, risk registers, audit reports, IT strategy plans, organizational charts, and reports from consultants and oversight bodies. These documents were selected to assess the formal structures, policies, and procedures governing IT risk and to evaluate their alignment with internationally recognized standards, particularly the Risk IT Framework developed by (ISACA, 2009). The analysis revealed several recurring gaps within NBE IT risk management approach, highlighting deficiencies in governance, policy formulation, and strategic alignment.

A key finding of this review was the absence of a dedicated IT risk governance structure. Currently, the Internal Audit and Risk Management Directorate (IARM) oversee general risk management functions; however, no formal IT risk committee or cross-functional governance body exists to provide specialized oversight (NBE, 2023). This governance gap results in a fragmented approach to IT risk management, lacking a clear line of accountability for IT-specific risks. Furthermore, the review found that NBE lacks a standalone IT risk management policy. While general risk management frameworks are in place, they do not provide detailed guidance on identifying, assessing, responding to, or continuously monitoring IT risks (IMF, 2020). The

absence of a comprehensive IT risk policy makes risk management practices reactive rather than proactive, limiting the institution ability to mitigate emerging threats effectively.

Additionally, broad institutional risk appetite statements exist, but they are not translated into specific IT risk tolerance thresholds. Consultant reports highlight inconsistencies in risk perspectives across departments, resulting in a lack of alignment in risk prioritization and mitigation strategies (Deloitte, 2016). This disjointed approach further extends to financial planning, where budgetary and planning documents fail to establish a clear linkage between IT risk priorities and resource allocation (World Bank,, 2024). Without structured financial investment in IT risk mitigation, critical vulnerabilities remain unaddressed. External audits and technical assistance reports from the International Monetary Fund (IMF) emphasize the need to establish an IT risk committee and update IT risk policies, yet implementation has been partial or absent (IMF, 2020).

When assessed against the three domains of the Risk IT Framework Risk Governance, Risk Evaluation, and Risk Response these findings reveal significant gaps in NBE IT risk management approach (ISACA, 2009). The lack of a structured governance mechanism, the absence of a dedicated IT risk policy, and the failure to integrate risk considerations into financial planning underscore the necessity of a comprehensive IT Risk Management Framework tailored to the NBE context. Addressing these gaps requires a structured approach that aligns with international best practices, strengthens governance mechanisms, and ensures effective risk evaluation and response strategies (Basel Committee on Banking Supervision, 2019). The proposed framework should incorporate clear governance structures, standardized risk assessment methodologies, and proactive risk mitigation strategies to enhance the resilience of Ethiopia’s banking sector.

4.4. Discussion

4.4.1. What are the challenges to manage IT risks in the National Bank of Ethiopia?

The study revealed a range of critical challenges confronting the National Bank of Ethiopia in managing IT risks effectively. These challenges were identified through a triangulation of qualitative interview data, internal document review, and an alignment with established literature on IT risk management within the banking sector, particularly in developing and emerging economies.

A primary challenge identified is the lack of a dedicated IT risk governance structure. The document review revealed that while the Internal Audit and Risk Management Directorate (IARM) oversees general risk functions, there is no specialized IT risk committee or cross-functional governance body tasked explicitly with IT risk oversight (NBE., 2010). This governance vacuum is reflecting by the interviews, which highlighted unclear accountability for IT-specific risks. This finding aligns with the literature emphasizing governance as the foundation of effective IT risk management. According to ISACA (ISACA, 2009), Risk Governance is critical for establishing ownership, accountability, and alignment of IT risks with business objectives. (Basel Committee on Banking Supervision, 2019) similarly stresses that without formal governance, risk management becomes fragmented and reactive. In emerging economies, such gaps are commonly observed due to resource constraints and evolving organizational maturity (Deloitte, 2016).

The absence of clear governance mechanisms at NBE inhibits coordinated decision-making and weakens strategic risk oversight, a major impediment to proactive IT risk management. The research further highlights that despite recommendations from international oversight bodies such as the IMF and consultant reports advocating for the establishment of IT risk committees and updated policies, implementation has been partial or lacking. The failure to act on these recommendations perpetuates existing vulnerabilities and undermines the development of a mature IT risk management culture at NBE.

One of the most pervasive internal challenges identified is the shortage of skilled personnel in IT risk and cyber security domains. This issue is consistently highlighted in global and local assessments. For instance, (World Economic Foroum, 2020) and (Kaspersky, 2023) both emphasize Ethiopia limited cyber security and IT risk management expertise, a situation exacerbated at NBE by a dependence on expensive external consultants. (IMF, 2020), also noted that limited human resource capacity in regulatory institutions extends to the area of IT risk oversight.

Interview responses further confirmed these systemic gaps. Participant 1 stated, “The absence of well-equipped talent and regular training makes it difficult to adopt or maintain new technologies. As a result, vulnerabilities are not easily identified.” Participant 6 reflected this view, pointing out that the lack of continuous training significantly undermines the Bank’s

capacity to address evolving technological threats. These observations align with (Carcary, 2012), who argues that the presence of skilled human capital is fundamental for effective IT governance and risk management. Without a sustained investment in capacity-building, organizations are unlikely to keep pace with rapid technological change or proactively identify and respond to emerging risks, thereby increasing the likelihood of operational, reputational, and regulatory exposure.

A further critical challenge identified in the study is the absence of a dedicated and comprehensive IT risk management policy at the National Bank of Ethiopia. While some draft frameworks are in place, they remain overly generic and fail to provide clear, actionable guidance on essential risk management processes such as IT risk identification, assessment, monitoring, and mitigation. This policy gap has resulted in a reactive rather than proactive approach to managing IT risks, where responses are often triggered by incidents rather than guided by preventive strategies. This finding aligns with the (IMF, 2020), which emphasizes that the lack of tailored IT risk policies undermines an institution's ability to operationalize risk management effectively. Similarly, (Carcary, 2012) underscores the importance of formalized policies in fostering a consistent risk management culture and ensuring accountability across financial institutions. The fragmentation caused by the lack of a unified policy is also evident in internal audit reports and risk registers reviewed during the study, which show inconsistent practices and unclear ownership of IT risk activities.

Interview data reinforced these concerns. For instance, Participant 2 remarked, "We don't have a dedicated IT risk policy what we follow is part of a general risk framework that doesn't address the unique nature of IT-related threats." Likewise, Participant 5 observed, "Because there is no clear guideline, teams tend to address IT risks on an ad hoc basis, depending on urgency rather than following a structured plan." These insights illustrate how the absence of a formal IT risk policy hampers the integration of risk management into daily operations, weakens compliance with controls, and limits the institution's overall resilience to technology-related threats. Therefore, establishing a well-defined and context-specific IT risk policy is essential for strengthening NBE risk governance and aligning its practices with international standards. What is the current status of IT risk management practice in National Bank of Ethiopia?

Another recurring concern was the prevalence of legacy systems and outdated infrastructure. These systems were described as inefficient, difficult to integrate with modern solutions, and prone to failure. Participant 1 noted that "reduced efficiency, higher maintenance costs, and limited scalability" were among the consequences of operating such systems. Participant 9 added that outdated infrastructure severely limits the bank's ability to respond swiftly to market or regulatory changes, leading to reduced productivity and elevated operational risk. The literature supports these concerns. (ISACA, 2009), warns that aging infrastructure often undermines agility, resilience, and security critical attributes in an increasingly digital banking environment. Effective IT risk management requires modern, well-maintained systems that support proactive monitoring, fast response, and scalability.

The literature highlights cyber threats, regulatory changes, and rapid digitalization as significant challenges. (Tadesse, 2024) and (Bank for International Settlements, 2023), note the rising frequency of cyber-attacks like phishing and ransomeware, particularly in developing economies with limited cyber security infrastructure. (European Central Bank (ECB) Supervision, 2024) further stress the NBE struggle to align with international standards like the Digital Operational Resilience Act (DORA) due to resource constraints. Interview data indirectly supports these findings by highlighting outdated infrastructure and a lack of proactive incident management These challenges were further reflected in the interview data. Participant 1 explained, "We are still operating with outdated infrastructure, which makes us more exposed to modern cyber threats. Our response is usually after the fact, not before." Similarly, Participant 4 noted, "There is no centralized or automated system for detecting incidents early; most issues are identified manually or too late." These statements reveal critical gaps in the Bank's ability to identify and respond to cyber threats in a timely manner. (Policy Studies Institute, 2024), also points to fintech-driven risks, such as those from platforms like Telebirr, which the NBE struggles to regulate due to infrastructure deficiencies. These findings collectively highlight a complex risk landscape that the proposed ITRM framework must address, tailored to the NBE resource-constrained environment.

4.4.2. What is the current status of IT risk management practice in National Bank of Ethiopia?

The current status of IT risk management (ITRM) at the National Bank of Ethiopia is characterized by a fragmented and informal structure that lacks specialization and strategic coordination. Responsibility for IT risk currently resides within the Internal Audit and Risk Management Directorate (IARM), which oversees various types of organizational risk but does so without IT-specific expertise or personnel (NBE., 2010). As such, IT risks are managed under a generalized framework, with no dedicated IT risk governance body, such as an IT risk committee or cross-departmental working group. This governance gap is echoed by Participant 2, who noted, "There is no centralized risk management structure that oversees IT risks comprehensively. Each department addresses issues reactively, and there's no shared strategy."

Similarly, Participant 7 emphasized the lack of accountability, stating, "IT risk issues are not getting the attention they deserve. The structure doesn't support accountability or communication between IT and risk units." These internal insights align with (Carcary, 2012) and (Deloitte, 2016) observations that in many developing economies, IT risk is often embedded within broader audit functions, resulting in a lack of specialized processes, ownership, and strategic oversight. Furthermore, the absence of IT-specific personnel within IARM reinforces the challenge of implementing proactive and technically informed IT risk responses. Without clear structures and specialized resources, the bank current ITRM practice remains reactive, silos, and poorly aligned with best practices advocated in international frameworks, such as (ISACA, 2009), which calls for dedicated roles, continuous evaluation, and governance mechanisms. Therefore, it is evident that the existing practice at NBE lacks the foundational components necessary for effective and resilient IT risk management.

4.4.3. What are the key processes essential for IS/IT risk management framework?

The development of a tailored Information Systems Risk Management framework(ISRMF) for the National Bank of Ethiopia requires identifying key processes that address its unique challenges while aligning with global best practices. These processes address internal challenges, such as policy gaps, fragmented governance, and outdated infrastructure, and external pressures, including cyber threats and regulatory changes, ensuring alignment with the NBE's strategic objective of enhancing financial sector stability.

Establishing a common risk view is foundational to an effective IS/IT risk management framework. The literature emphasizes the critical role of clearly defined governance structures in aligning IT risk management with broader organizational objectives (Jordan & Silcock, 2005; ISACA, 2009). However, at the National Bank of Ethiopia , the absence of a formal governance framework significantly hinders this alignment. As Participant 1 explained, “Our organization has not yet aligned its IT risk management activities due to the absence of an approved ERM framework and clearly defined roles.” This view is reinforced by Participant 5, who noted, “No formal IT risk framework has been developed to reflect the bank’s overarching strategic objectives.” Business unit perspectives also confirm this gap. For example, Participant 9 observed, “There is no structured engagement between IT and strategic planning teams,” while Participant 10 highlighted the lack of defined IT risk thresholds.

The governance challenge is further exacerbated by the absence of a dedicated IT risk oversight body. As Participant 7 stated, “The bank lacks an established governance framework or committee specifically for IT risk oversight.” Moreover, fragmented risk perceptions persist even within technical teams, with Participant 3 noting, “There is not a common perception, even within technical teams.” These insights reveal a fragmented and inconsistent understanding of IT risk across the institution. Addressing this requires the establishment of a centralized IT risk committee, the development of standardized IT risk management policies, and the definition of a risk appetite aligned with NBE mission and strategic objectives. Doing so directly addresses Specific Objective 1 of this study reviewing existing frameworks by applying principles from the ISACA Risk IT Framework, and supports Specific Objective 3 proposing a tailored framework by responding to the specific governance challenges observed at NBE.

Integrating IT risk with Enterprise Risk Management (ERM) is essential for ensuring a holistic and coordinated approach to risk governance, as emphasized by Risk IT governance objective RG2 (Integrate with ERM). The literature underscores that embedding IT risks within enterprise-wide strategies is critical to prioritizing risk mitigation efforts effectively and consistently (Van Grembergen, 2009). However, at the National Bank of Ethiopia, the absence of a centralized and formally approved ERM framework has led to fragmented and siloes IT risk practices. As Participant 4 observed, “Risk management practices are distributed, and there is no centralized ERM framework that includes IT risk as part of the broader enterprise risk profile.” This concern

was echoed by Participant 7, who noted, “The absence of an approved ERM framework results in IT risks being managed separately, which can lead to inconsistencies in risk prioritization.”

Further reinforcing this gap, business unit respondents highlighted procedural limitations and lack of formal integration. Participant 9 stated, “The ERM framework remains in draft form and has yet to receive formal approval from management,” while Participant 10 added, “IT-related issues are recorded manually… their integration into general operational risk reports is informal.” These observations reflect a critical weakness in strategic alignment, where IT risk is not systematically incorporated into enterprise-level risk oversight.

To address this, it is imperative to develop and institutionalize a centralized ERM framework that explicitly integrates IT risk registers and promotes structured collaboration between the Information Systems Management Directorate (ISMD), Internal Audit and Risk Management Directorate (IARMD), and relevant business units. This process supports the broader objective of enhancing financial sector stability through integrated risk management and aligns with the strategic goals of the bank as well as the Risk IT Framework’s principles.

Risk-aware decision-making, aligned with Risk IT governance objective RG3 (Make risk-aware business decisions), is vital for ensuring that IT investments support and advance organizational strategic goals. The literature emphasizes that strategic decisions should be informed by risk intelligence to foster resilience and value creation (Kaplan, 2012). However, at the National Bank of Ethiopia, decision-making processes are predominantly compliance-driven rather than strategically risk-informed. As Participant 2 explained, “Business decisions are shaped more by compliance requirements than by internally driven IT risk evaluations.” This observation was further supported by Participant 1, who noted, “The risk department does not provide concrete or structured reports to senior leadership to support decisions on upgrading systems.”

Business unit participants echoed these concerns, highlighting a lack of consultation and reactive practices. Participant 9 stated, “Business units responsible for managing IT risks are rarely consulted,” while Participant 11 pointed to budgeting decisions being driven by short-term financial pressures rather than long-term risk considerations. These findings reveal a significant gap in incorporating risk insights into business planning, which undermines proactive IT governance. Addressing this issue requires the development and implementation of structured,

timely, and relevant risk reporting mechanisms that inform strategic investments particularly in areas such as digital payment platforms and vendor management. This aligns with Specific Objective 2 by critically examining existing reactive practices, and supports Specific Objective 3 by laying the groundwork for a proposed framework that enables risk-informed decision-making across the institution.

Collecting IT risk data is a foundational activity in the risk identification process, corresponding to Risk IT RE1 (Collect data). The literature underscores the importance of automated and centralized data collection mechanisms to enable timely, accurate, and proactive risk identification (NIST., 2012). At the National Bank of Ethiopia, however, risk data collection remains largely fragmented and manual. As Participant 2 observed, "IT risk data is recorded in separate registers across departments, leading to data silos, inconsistent formats, and limited visibility." This silos approach inhibits holistic risk oversight and undermines timely response.

Moreover, risk data updates are infrequent and lack standardization. Participant 1 noted, "The risk department sends to business units to update the risk registry annually," while Participant 4 highlighted a more serious gap: "There is no standardized risk register, and potential threats are not consistently logged or tracked." Business unit feedback P10 also confirmed that IT risk information is not systematically integrated into operational risk reporting, further weakening visibility and coordination.

While there is some collaboration with external agencies such as the Information Network Security Administration (INSA) Participant 2 emphasized that "The IT Security team collaborates with INSA to identify emerging risks," indicating potential for improvement through inter-agency support. Nevertheless, establishing a centralized and automated IT risk register is imperative for overcoming data silos and enabling proactive risk identification, particularly within NBE resource-constrained operational environment. This also directly supports Specific Objective 2 (exploring current practices) and Specific Objective 3 (proposing a framework) through enhanced data governance and risk visibility.

Analyzing IT risks is vital for effective prioritization and aligns with Risk IT RE2 (Analyze Risk). The literature emphasizes the importance of using advanced methodologies and skilled personnel to assess complex and evolving IT threats (ISO, 2018). At the National Bank of

Ethiopia, however, current practices rely on overly simplistic tools that limit the effectiveness of risk analysis. As Participant 1 explained, “The risk department uses a simple categorization approach in the risk register, classifying risks as ‘high, medium, and low,’” a method that lacks the granularity required to address today’s sophisticated threat landscape. This concern was echoed by Participant 8, who noted, “These classifications may not align with the complexities of modern IT threats.”

Moreover, the quality of analysis is undermined by limited expertise. Participant 2 pointed out, “Assessments are conducted by personnel who lack specialized IT risk expertise,” while business unit respondents, P9 and P10 confirmed the absence of structured processes for evaluating emerging risks. Despite some progress through external collaboration such as the IT Security team partnership with INSA to collect audit data, security reports, and monitor industry trends Participant 6 these efforts remain ad hoc and lack formal institutionalization. To strengthen risk analysis, NBE must adopt more sophisticated tools such as probability-impact matrices, and scenario analysis. Equally important is the development of internal capacity through targeted training in IT risk evaluation. These improvements directly contribute to Specific Objective 3 by ensuring that the proposed Information systems risk management framework is both context-sensitive and capable of addressing the complexity of risks faced by the Bank.

Maintaining a dynamic IT risk profile, in alignment with Risk IT RE3 (Maintain Risk Profile), is essential for effectively responding to the rapidly evolving threat landscape, particularly within fintech ecosystems. The literature underscores the need for continuous monitoring and real-time updates to risk profiles to ensure resilience and adaptability (ISACA, 2009). However, at the National Bank of Ethiopia, the current approach remains static and reactive. As Participant 1 acknowledged, “We are currently lagging behind the global financial sector in terms of updating and maintaining our IT risk profile,” While Participant 5 added, “The risk profile is not dynamically updated.”

This concern is echoed by business unit respondents. P9 highlighted that “Internal policies and systems are not keeping pace,” and P10 confirmed the absence of a centralized, regularly updated profile. Instead of proactive risk tracking, NBE predominantly relies on periodic audits and external enforcement. Participant 7 cited dependence on periodic reviews, while Participants 2 and 6 pointed to the role of INSA in identifying emerging risks, rather than internal systems

performing this function independently. To overcome these limitations, NBE must implement real-time monitoring mechanisms and structured, continuously updated profiling processes. This will ensure the organization remains agile in managing risks associated with fintech growth and increasing cyber threats. Such improvements directly support Specific Objective 3 by contributing to the design of a responsive and forward-looking IT risk management framework tailored to NBE evolving risk environment.

Effective risk communication, aligned with Risk IT RR1 (Articulate Risk), is vital for ensuring stakeholder awareness and informed decision-making across all levels of the organization. The literature highlights the importance of clear, tailored reporting mechanisms that translate complex IT risk information into formats understandable to non-technical stakeholders (COBIT 5, 2012). At the National Bank of Ethiopia, however, risk communication remains largely reactive and fragmented. As Participant 6 observed, “There is no indication of structured communication strategies or tailored reporting,” while Participant 1 emphasized, “The level of communication is very low.”

Business unit representatives echoed these concerns, citing difficulties in interpreting IT risk reports due to overly technical language. For example, P10 noted, “IT-related threats are frequently described using technical language,” which inhibits broader organizational understanding and engagement. This communication gap not only reduces the effectiveness of risk awareness but also limits the integration of risk considerations into strategic and operational planning. To address these challenges, NBE must develop standardized, accessible communication protocols that facilitate cross-functional understanding. This includes implementing tailored reporting templates, regular briefings, and training programs aimed at bridging the gap between technical and business perspectives. These enhancements respond directly to Specific Objective 2 by identifying and addressing the current shortcomings in risk communication practices within the Bank.

Proactive risk management, as outlined in Risk IT RR2 (Manage Risk), demands the implementation of diversified and structured response strategies. The literature underscores the need for formalized mechanisms such as risk mitigation, acceptance, and transfer to address the dynamic nature of IT risks effectively (ISO/IEC 27005, 2011). However, at the National Bank of Ethiopia, the current approach remains largely reactive and limited in scope. As Participant 1

remarked, “Mitigation is pursued particularly for well-known or previously experienced risks,” highlighting a narrow focus on familiar threats. Participant 6 further emphasized the lack of strategic diversification, stating, “There is no indication of formal use of risk transfer (e.g., cyber insurance).”

Business unit representatives, P9 and P11 also noted minimal involvement in risk response planning, citing reactive budgeting practices and limited cross-functional engagement. This fragmented approach hinders the institution’s ability to respond comprehensively to emerging and complex IT risks.To address these shortcomings, NBE must adopt a formalized risk response framework that incorporates mitigation, acceptance, and transfer strategies tailored to its operational context. Strengthening cross-departmental collaboration and exploring tools such as cyber insurance will be critical to enhancing the Bank’s overall resilience. This initiative directly supports Specific Objective 3 by proposing improvements that align IT risk management practices with the Bank’s broader strategic goals.

Responding effectively to IT incidents, in line with Risk IT RR3 (React to Risk Events), necessitates structured and predefined response plans. The literature underscores the importance of formalized incident response frameworks to ensure timely, coordinated, and efficient handling of Information system disruptions (NIST., 2012). At the National Bank of Ethiopia, however, responses remain largely reactive and informal. For example, Participant 5 stated, “We isolate affected systems by disconnecting external ports,” illustrating ad hoc containment efforts during crises such as the storage system failure. Participant 4 further noted that infrastructure vulnerabilities were exposed during the disaster recovery (DR) site fire, pointing to a lack of preparedness.

Moreover, business unit representatives, P10 and P11 reported minimal involvement in incident response activities, indicating insufficient coordination across departments. While collaboration with the Information Network Security Administration (INSA), as highlighted by Participant 1 and escalation to senior management Participant 2 provide some level of support, these measures are not embedded within a formalized incident management framework. To enhance resilience and ensure a systematic approach to future disruptions, NBE must prioritize the development and implementation of comprehensive incident response plans. These should be supported by regular training, infrastructure upgrades, and clearly defined roles and escalation protocols. Such

improvements directly contribute to achieving Specific Objective 3 by strengthening the Bank capacity to respond proactively and effectively to IT risk events.

4.5. IS/IT risk management for National bank of Ethiopia

4.5.1. Framework overview

IT/IS Risk Management Framework for the National Bank of Ethiopia is designed as an integrated, cyclical model that aligns IT risk management with the institution strategic business objectives. It is centered on a Core Element Business Objectives and structured around three interdependent domains: Risk Governance, Risk Evaluation, and Risk Response. These domains are interconnected through a continuous communication and feedback loop, which ensures adaptability, accountability, and ongoing alignment with both organizational priorities and the evolving external risk environment.

Business Objectives

At the center of the framework lies the foundational concept of Business Objectives. All IT risk management efforts are geared toward supporting and protecting these objectives, which reflect the National Bank of Ethiopia overarching goals: ensuring financial system stability, maintaining operational continuity, achieving regulatory compliance, and safeguarding institutional reputation and stakeholder trust.

By embedding business objectives at the core, the framework ensures that IT risk management is not merely a technical function but a strategic enabler. Each decision and control mechanism is evaluated based on how well it contributes to the Bank mission and strategic direction. Surrounding this core is a continuous communication loop, ensuring that risk data, evaluations, and response strategies are constantly aligned with changing internal and external conditions. This reinforces the agility of the risk management process and promotes strategic responsiveness.

Domain 1: Risk Governance

Risk Governance serves as the strategic cornerstone of the framework, aiming to embed IT risk management within the bank's overall governance and strategic structures. It ensures executive oversight, clear accountability, and alignment with enterprise risk management (ERM). This

domain promotes a culture where IT risk is not confined to technical units but recognized as a critical business risk with enterprise-wide implications, supported by active leadership involvement and well-defined risk responsibilities.

Key Processes:

1. Establish Robust Governance Structures
   Dedicated IT risk committees, supported by executive and cross-functional members, are essential to oversee and guide IT risk activities.
2. Make Risk-Aware Business Decisions
   IT risk must be factored into both strategic planning and day-to-day decision-making, allowing for more informed and holistic risk trade-offs.
3. Integrate IT Risk with ERM
   The IT risk function should be closely linked with the overall ERM framework, enabling a cohesive view of all risks across the enterprise.

Domain 2: Risk Evaluation

Risk Evaluation acts as the core analytical component of the framework, facilitating a systematic process for identifying and assessing risks. Utilizing reliable data and effective evaluation methods, this domain provides decision-makers with clear, prioritized information about risks. This enables them to make well-informed choices regarding risk responses and the allocation of resources. Its primary purpose is to identify, evaluate, and rank IT risks based on their probability, potential impact, and alignment with organizational goals.

Key processes:

1. Collect Data
   Gather information from audits, incident reports, threat intelligence feeds, operational logs, and external benchmarks.
2. Analyze and Prioritize Risks
   Use tools such as risk matrices, heat maps, and scoring mechanisms to evaluate the probability and business impact of each risk.

3. Maintain a Dynamic Risk Profile
   continuously update the risk register as threats evolve, vulnerabilities emerge, or business processes change.

Domain 3: Risk Response

Risk Response puts the insights gained from risk evaluations into action by implementing concrete measures that safeguard the organization, reduce risk exposure, and enhance resilience. This domain ensures that risk management is both proactive and reactive, enabling the National Bank of Ethiopia (NBE) to respond promptly to incidents while continuously strengthening its overall risk posture. Its purpose is to carry out efficient and effective actions to mitigate, transfer, accept, or avoid IT risks based on well-informed decisions.

Key processes:

1. Define Risk Response and Communicate to Stakeholders
   Develop response strategies and ensure they are communicated clearly to all relevant departments and individuals.
2. Prepare and Respond to Risk Events
   Establish and test incident response procedures, disaster recovery plans, and business continuity strategies to handle disruptions effectively.
3. Manage Risk Continuously
   Implement controls, track performance, evaluate their effectiveness, and revise response strategies as required to stay within acceptable risk thresholds.

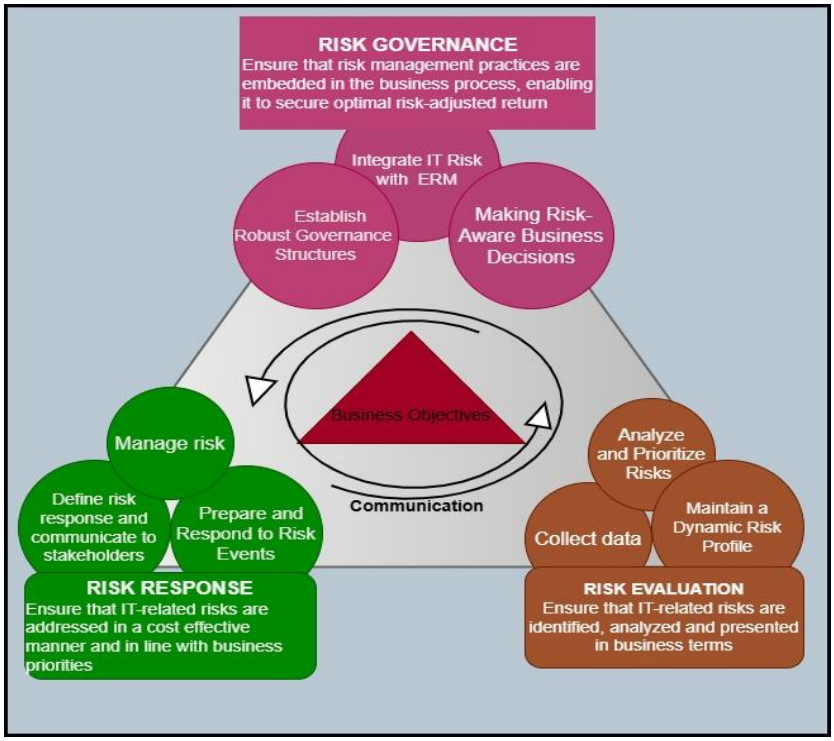
Communication and Continuous Feedback

A unique strength of this framework lies in its continuous communication and feedback loop, represented by a circular interaction among the three domains. This dynamic mechanism ensures:

- Governance directives inform risk evaluation focus areas and organizational risk appetite.
- Evaluation outputs guide risk response planning and prioritization.
- Response outcomes and control performance are feedback to refine governance policies and strategic objectives.

This closed-loop approach facilitates agility, transparency, and continuous learning, all of which are vital in the dynamic environment of IT risk.

Figure 5: Proposed Information system Risk management frameworks.



4.5.2. **Framework evaluation responses**

A qualitative content analysis was conducted to evaluate expert feedback on the proposed IT Risk Management Framework for the National Bank of Ethiopia. Insights were obtained from three senior professionals with expertise in IT Supervision and a solid understanding of international standards such as the Risk IT Framework. The analysis identified recurring themes across four key dimensions: relevance, comprehensiveness, practicality, and alignment with best practices.

Relevance

Across the board, the experts confirmed the high relevance of the proposed framework to NBE current IT risk context. A central theme that emerged was the recognition of structural fragmentation and the absence of enterprise-wide coordination in existing IT risk practices. To begin with, Participant One observed that the framework accurately captures misalignments

between operational IT functions and enterprise risk oversight, a gap that has historically undermined risk management at NBE.

Similarly, Participant Two stressed that the framework is well aligned with NBE's existing risk maturity level, making it both timely and necessary for the institution. In addition, Participant Three pointed out that the framework plays a crucial role in clarifying risk ownership, a responsibility that is often ill-defined in traditional risk models. Taken together, these insights underscore that the framework is not only contextually appropriate but also effectively addresses key organizational deficiencies within NBE IT risk landscape.

Comprehensiveness

When evaluating comprehensiveness, the experts collectively praised the framework holistic coverage of the IT risk management lifecycle. Specifically, they appreciated the inclusion of all core components: risk governance, identification, assessment, response, and continuous monitoring. However, two recurring areas for improvement were raised. First, Participant Two noted the absence of defined performance measurement tools, such as Key Performance Indicators (KPIs) and maturity models, which are essential for tracking progress and evaluating effectiveness.

Additionally, Participant Three emphasized the need for procedural implementation guidance, arguing that without such detail, the framework may face challenges in operationalization.

Furthermore, both participants agreed that incorporating these elements would significantly enhance the framework's measurability, usability, and institutional effectiveness. Thus, while the framework demonstrates strong foundational coverage, the addition of performance metrics and procedural detail would enhance its completeness and functional value.

Practicality

Regarding practicality, the experts consistently described the framework as implementable within NBE's current structure and resource constraints. A central theme here was the modular and phased design, which allows for gradual rollout and scalability. In support of this, Participant Two highlighted that the framework step-by-step structure is particularly suited for environments with limited resources, enabling more realistic and manageable adoption. Conversely, Participant Three cautioned that successful implementation will require strong executive sponsorship and

cross-functional collaboration, noting that organizational buy-in is critical to overcome potential resistance or silos.

Moreover, all three experts agreed on the importance of capacity building and training, as the Bank limited in-house IT risk expertise could otherwise hamper long-term sustainability. In summary, while the framework is seen as practically feasible, its success will be contingent on institutional commitment, staff development, and strategic coordination.

Alignment with Best Practices

The final theme alignment with international best practices received unanimous support. The experts agreed that grounding the framework in established standards the Risk IT provides a strong foundation of credibility and future-readiness. For instance, Participant One pointed out that this alignment not only enhances the framework's legitimacy within NBE, but also positions it for adoption by other public institutions facing similar challenges.

Similarly, Participant Three emphasized the framework flexibility and adaptability, asserting that it is well-prepared to accommodate evolving technologies and regulatory shifts. Consequently, the framework's alignment with globally recognized frameworks reinforces its scalability, compliance potential, and long-term sustainability.

To enhance the framework's practical applicability, the following actionable recommendations are proposed:

- Introduce performance measurement tools (e.g., KPIs and maturity models)
- Develop detailed procedural implementation guidance.
- Adopt a phased rollout strategy to manage change incrementally,
- Ensure executive sponsorship and interdepartmental cooperation to foster collective ownership and accountability.

4.5.3. NBE IT Risk Management Framework Implementation Roadmap

Phase 1 Foundation (0–6 months)

- Establish dedicated IT risk management function within the bank
- Approve IT risk management policy and define IT risk appetite statement

- Form IT Risk Governance Committee involving key stakeholders (ISMD, IARM, business units, senior management).

Phase 2 Evaluation Setup (6–12 months)

- Develop and populate IT risk register with identified risks across units
- Define and implement risk assessment methodology and processes
- Conduct staff training and roll out IT risk awareness programs bank-wide
- Procure and deploy risk management tools and technologies for assessment and monitoring

Phase III – Operationalization (12–18 months)

- Launch comprehensive IT risk response procedures (mitigation, transfer, acceptance, avoidance)
- Initiate regular IT risk reporting to senior management and board-level committees
- Institutionalize continuous feedback mechanisms and periodic framework reviews for ongoing improvement

CHAPTER FIVE
SUMMARY OF KEY FINDINGS, CONCLUSION RECOMMENDATIONS AND FUTURE WORKS

5.1.Summary of Key Findings

This study investigated the current status of IT risk management practices at the National Bank of Ethiopia and identified key processes essential for a tailored Information Systems Risk Management (ISRM) framework, guided by ISACA's Risk IT Framework (ISACA, 2009). The findings, derived from semi-structured interviews with NBE stakeholders and a comprehensive literature review, reveal significant internal and external challenges, fragmented practices, and critical processes necessary to enhance the NBE IT risk management capabilities. These insights address the study's objectives of reviewing global frameworks, exploring NBE practices, and proposing a context-specific ISRM framework to support financial sector stability in Ethiopia's evolving digital landscape.

This study examined the current IT risk management practices at the National Bank of Ethiopia , revealing a predominantly reactive and fragmented approach. The absence of a standalone IT risk management policy aligned with the bank's strategic objectives was a significant finding. Interview data showed that existing frameworks are generic and do not proactively address emerging IT risks. Furthermore, the lack of a formal Enterprise Risk Management (ERM) framework contributes to silos operations and inconsistent perceptions of IS risks across departments. Governance structures dedicated to IT risk oversight are notably absent, limiting coordination and accountability. Data management remains manual and decentralized, leading to limited visibility and inconsistent reporting. Risk analysis methods are simplistic and misaligned with the evolving IT risk landscape, including emerging threats such as fintech vulnerabilities. Incident responses are largely ad hoc, illustrated by infrastructure failures like the data recovery site fire caused by power leakage. These findings highlight critical gaps that impede effective IS risk management within NBE and underscore the need for more integrated, strategic, and proactive risk governance.

The study also revealed a combination of internal and external challenges that hinder the National Bank of Ethiopia Information system risk management capabilities. Internally, critical issues include a shortage of skilled IT risk professionals, outdated infrastructure, and weak governance. Participants emphasized that Information system risk assessments are often performed by inadequately trained personnel, and risk mitigation tends to focus on previously encountered threats using basic controls. Externally, increasing cyber threats such as phishing and ransomware exploit existing system vulnerabilities, prompting reliance on the National Cyber Emergency Response Team for support. Additionally, compliance with externally enforced cyber security regulations such as those mandated by INSA places further strain on institutional resources. These findings align with regional research highlighting Ethiopia limited cyber expertise and infrastructure deficits, reinforcing the urgency of establishing a more resilient and strategically managed ISRM framework.

The key findings of the study, which investigated the foundational processes required to develop an effective Information Systems Risk Management (ISRM) Framework for the National Bank of Ethiopia (NBE). Structured according to the ISACA Risk IT Framework domains:- Risk Governance (RG), Risk Evaluation (RE), and Risk Response (RR). The chapter identifies nine critical processes underpinning a robust ISRM approach. Under Risk Governance, the study revealed the absence of a formal governance structure and the lack of integration between IT risk and enterprise risk management, resulting in fragmented oversight and weak accountability. Within Risk Evaluation, significant challenges were identified in the collection, consolidation, and analysis of IT risk data due to silos systems and limited analytical tools, impairing timely and informed decision-making. The Risk Response domain highlighted inconsistencies in defining and communicating risk responses, a predominantly reactive approach to risk events, and a lack of continuous risk monitoring mechanisms. These findings were supported by direct insights from participant interviews and demonstrate a significant gap between NBE current practices and international standards such as ISO/IEC 27005 and NIST SP 800-39. Furthermore, the study contextualizes these challenges within the Ethiopian banking environment, marked by constrained resources, evolving digital capabilities, and a growing need for risk management capacity building. Ultimately, the findings underscore the need for a localized yet globally aligned ISRM Framework to enhance NBE strategic response to IT-related risks.

The findings reveal a critical need for a structured, proactive ISRM framework to address the NBE's fragmented practices and vulnerabilities. The absence of policies, governance, and integrated processes, coupled with external pressures, undermines the NBE ability to manage IT risks effectively. The identified processes provide a roadmap for enhancing risk management, supporting the study's objective of proposing a context-specific framework to strengthen financial sector stability.

5.2. Conclusion

The main objective of this research was to assess the current IT risk management practices at the National Bank of Ethiopia, identify existing gaps, and propose possible improvements based on international best practices and frameworks.

This study employed a qualitative approach, utilizing in-depth interviews with key stakeholders and document analysis to evaluate the extent to which the bank IT risk management aligns with recognized standards and strategic objectives. The findings reveal that NBE currently lacks IT risk management policy, and its risk management approach continues to be primarily ad hoc and uncoordinated. While some basic risk identification and categorization processes exist, they are insufficiently aligned with the evolving IT risk landscape and do not effectively incorporate emerging risks such as fintech vulnerabilities.

Moreover, governance deficiencies were observed, including the absence of a dedicated IT risk management committee and fragmented data collection mechanisms that hinder comprehensive risk visibility and coordination. Incident response processes, such as those following the recent disaster recovery site fire, were found to be ad hoc and uncoordinated, underscoring weaknesses in infrastructure resilience and preparedness.

In conclusion, addressing these gaps through the development of comprehensive policies, enhanced governance structures, and targeted capacity building is critical for improving the effectiveness of IT risk management at NBE. This will enable the bank to better anticipate, identify, and respond to IT risks in a strategic and proactive manner.

5.3. Limitations

This study has several limitations that should be considered when interpreting the findings:

The research focused solely on the National Bank of Ethiopia, which may limit the applicability of results to other financial institutions or sectors.

Data collection was based on interviews with selected staff and document review, which may introduce respondent bias and limit the breadth of perspectives.

The study relied on qualitative methods without extensive quantitative validation, which might affect the generalizability of the findings.

Rapid changes in technology and emerging risks mean that the identified gaps and recommendations could evolve over time, requiring ongoing reassessment.

5.4. Recommendations

In light of the findings, the following recommendations are proposed to strengthen IT risk management at NBE:

Develop and implement a comprehensive IT risk management policy that is explicitly aligned with the bank's strategic objectives and incorporates current and emerging IT risks.

Establish a dedicated IT risk governance committee or body to ensure coordinated oversight, accountability, and continuous review of IT risk management activities.

Integrate IT risk management within a formal Enterprise Risk Management (ERM) framework to promote cross-departmental collaboration and consistent risk perception.

Implement centralized and automated risk data collection and reporting tools to improve data quality, visibility, and facilitate real-time risk monitoring.

Adopt advanced risk assessment methodologies tailored to the evolving IT environment, including fintech and cyber security threats.

Develop and regularly test formal incident response and disaster recovery plans to enhance resilience and minimize the impact of IT disruptions.

Bibliography

NIST. (2018, JANUARY 14). Retrieved from http://www.nist.gov: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=904985]

A. Herrmann. (2013). The Quantitative Estimation of IT-Related Risk Probabilities,. *Society for Risk Analysis, 33*(8), 1510–1531,.

Adane, K. (2020). The Current Status of Cyber Security in Ethiopia. *The IUP Journal of Information Technology,*, 1-14.

Adebayo, O. &. (2021). Challenges in Enterprise Risk Management in Developing Economies. *Journal of Financial Regulation and Compliance,, 29*(3), 245-260.

African Development Bank, E. F. (2022). *https://www.afdb.org/en/countries/east-africa/ethiopia/ethiopia-economic-outlook*. Retrieved January 12, 2025, from https://www.afdb.org: https://www.afdb.org/en/countries/east-africa/ethiopia/ethiopia-economic-outlook

Ahlan, A. &. (2012, April 06). *Understanding components of IT risks and enterprise risk management. Enterprise risk management – A framework for success*. Retrieved April 25, 2012, from www.intechopen.com: DOI: 10.5772/32023

Ahmed sherif. (2024, april). *https://www.statista.com/*. Retrieved from statista: https://www.statista.com/statistics/203935/overall-it-spending-worldwide/

Al-Ahmad, W. &. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science,2(2)*, 28-43.

AlBahar, J. F. (2013). ystematic Risk Management Approach for Construction Projects. Journal ofConstruction Engineering and Management,. *116*(3), 533-546.

Alberts, C. A. (2003). *OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Carnegie Mellon Software Engineering Institute.

Allan, N. &. (2007). Strategic risk: It's all in your head. *ICE Proceedings Civil Engineering, 160,* 137-143.

Alter, S. &. (2004). A general, but readily adaptable model of information system risk. *Communications of the Association for Information Systems,, 14*(1), 1–28.

Amraoui, S. E. (2019). Information systems risk management: Literature review. *Computer and Information Science,, 12*(3), 1-1.

Anderson, R. &. (2020, feb 6). Retrieved 12 13, 2021, from Coso.org: https://www.iia.nl/SiteFiles/Publicaties/COSO-ERM-Creating-and-Protecting-Value.pdf;

Anikin, I. (2014). Based on AHP and Fuzzy Sets. *2nd Intl' Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM'2014).* Istanbul (Turkey).

Aven, T. &. (2014). "Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation". *European Journal of Operational Research.*

Azizi, N. & Hashim, K. (2010). Enterprise level IT risk management. *2010 3rd IEEE International Conference on. 3*, pp. 401-404. Chengdu, China: Computer Science and Information Technology (ICCSIT).

Babbie, E. (1998). *The Practice of Social Research.* Wadsworth Publishing..

Babu, M. S. (2013). *Enterprise Risk Management Integrated framework for Cloud Computing*, (Vol. 1950).

Bakshi, B. S. (2012). *Risk IT Framework for IT Risk Management : A Case Study of National Stock Exchange of India Limited*,.

Bank for International Settlements, C. a. (2023, June 11). *https://www.bis.org/fsi/publ/insights50.pdf*. Retrieved January 22, 2024, from https://www.bis.org: https://www.bis.org/fsi/publ/insights50.pdf

Barlette, Y., & Fomin, V. V. (2010). The adoption of information security management practices in SMEs. *Journal of Small Business and Enterprise Development,, 17*(4), 567-583.

Barrenechea. (2013, September 24). Information governance is good business. *Information governance is good businessOpentext CEO White Paper Series*, pp. 1-17.

Barrenechea, M. (2013). *Information governance is good business.* London: Opentext CEO White Paper Series.

Barua, A. K. (1995). Information technologies and business value: an analytical and empirical investigation. *Information Systems Research, 6*(1), 3-23.

Basel Committee on Banking Supervision, 2. (2019, Dec 15). *Supervisory Review Process: Risk Management (SRP30),Version Effective as of 15 Dec 2019*. Retrieved march 29, 2024, from BIS website: https://www.bis.org/basel_framework/chapter/SRP/30.htm

Bebbington, J. L. (2008). Corporate social reporting and reputation risk management. *Accounting, Auditing & Accountability, 21*(3), 337-361.

Bennett, M. J. (2017). Development model of intercultural sensitivity. In M. J. Bennett, *The International Encyclopedia of Intercultural Communication.* wiley: International encyclopedia of intercultural communication.

Bin Ishaq Alseiari, K. (2015, october 6). *eprints.glos.ac.uk*. Retrieved october 23, 2015, from eprints.glos.ac.uk: https://eprints.glos.ac.uk/id/eprint/2739

Biz. (2005). Compliance and the compliance function in banks. *Basel Committee on Banking Supervision*, 1-16.

Blakley, B. M. (2001). Information security is information risk management. *tNSPW '01 Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 97-104). New York, NY, United States: Association for Computing Machinery.

Bornman, W. (2008). *Information security risk management: a holistic framework.* Retrieved June 01 , 1992, from https://doi.org/10.1057/palgrave.jibs.8490270

Braun, V. &. (2006). Using thematic analysis in psychology. *Taylor & Francis., 3*(2), 77-101.

British Standards Institution. (2011, June 30). *Risk management – Code of practice and guidance for the implementation of BS ISO 31000*. Retrieved march 29, 2024, from www.apm.org.uk: https://www.apm.org.uk/media/1257/risk-appetite-and-risk-tolerance.pdf

Bryman, A. (2004). *Social Research Methods (2nd ed.).* . (4th ed.). Oxford: Oxford University Press.

Burtonshaw-Gunn, S. A. (2009). Risk and Financial Management in Construction. *Gower*.

Callon, M. L. (2001). Agir dans un monde incertain : . *Essai sur la démocratie technique.* Paris :: Editions du Seuil.

Campbell, D. T. (1963). *Experimental and quasi-experimental designs for research on teaching. In N. L. Gage (Ed.), Handbook of research on teaching.* Chicago: : Rand McNally.

Carcary, M. (2012). "IT Risk Governance: Building a Risk-Aware Culture". *Journal of Information Systems*.

Cassell, C. a. (2004). *Essential Guide to Qualitative Methods in Organizational Research.* Thousand Oaks.: Sage.

Cerchiello, P. G. (2016). Big data analysis for financial risk management. *Journal of Big Data, 3*(1), 237-255.

Chapman, R. J. (2011). Simple tools and techniques for enterprise risk management. *John Wiley & Sons, 553*.

Chris, E. (2024, February 29). *Compliance Risk Assessment Framework: A Comprehensive Guide*. Retrieved 5 8, 2024, from https://riskpublishing.com/: https://riskpublishing.com/compliance-risk-assessment-framework/

Chun, R. (2005). Corporate reputation:meaning and measurement. *International Journal of Management Reviews, 7*(2), 91–109.

Cindy Levy, E. L. (2010). *Taking of control organization risk culture.* London: McKinsey & Company.

Claudia Buch, C. o. (2024:, March). *https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240312~5990ccfce7.en.html*. Retrieved october 13, 2024, from https://www.bankingsupervision.europa.eu:

https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240312~5990ccfce7.en.html

COBIT 5, ISACA. (2012). *A business framework for the governance and management of enterprise IT.* Retrieved from Retrieved from www.isaca.org.

COBIT 5. (2012). *Enabling Processes.* ISACA.

Coertze, J. &. (2013). A model for information- security governance in developing countries, in K. Jonas, I.A. Rai & M. Tchuente (eds). E-infrastructure and e-services for developing countries. *International Conference on e-Infrastructure and e-Services for Developing Countries. 119*, pp. 279–288. Port Elizabeth, south africa: Springer.

Collins, J. &. (2003). Business Research. A Practical Guide for Undergraduate and Postgraduate Students. *Polgrave Macmillan.*

Commitee, K. (2016). *The King Code of Corporate Governance for South Africa 2016. .* Johannesburg: IODSA (Institute of Directors Southern Africa.

COSO, C. o. (2017). *Enterprise risk management.*

Covello, V. T. (1992). Risk communication: An emerging area of health communication research. *Annals of the international communications Associations*, 359-373.

D. Hillson, D. (2002). The risk breakdown structure(RBS) as an aid to effectives risk management. *Fifth European Project management conference* (pp. 19-20). France-sud: Project management Professional Solutions limited.

D. Shaun, a. K. (2016, August 22,). *Effects of Information Technology Risk Management and Institution Size on Financial Performance.* Retrieved september 29, 2024, from https://scholarworks.waldenu.edu/dissertations/2636/: https://scholarworks.waldenu.edu/dissertations/2636/

Damodaran, A. (2008). Strategic Risk Taking: A Framework for Risk Management. Philadelphie, USA: Wharton School Publishing.

Damonte, R. (2016). IT risk assessment: Developing and defining the IT risk assessment process framework in the case company. *Helsinki Metropolia University of Applied Sciences.*

Debreceny, R. (2013). Research on IT Governance , Risk , and Value : Challenges and Opportunities,. *JOURNAL OF INFORMATION SYSTEMS, vol. 27*,(No. 1), 129–135.

Degu Kefale Chanie, K. M. (2024). Assessment of Financial and Social Disclosure Level of Ethiopian Commercial Banks. *Humanities and Social Sciences Communications, 11*, 402.

Deloitte. (2016). *Information technology risks in financial services: What board members need to know and do*. Retrieved from deloitte: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-information-technology-risk-in-fs.pdf.

Denzin, N. K. (1970). *The Research Act:A Theoretical Introduction to Sociological Methods.* New York: by Norman K.Denzin.

Dhillon, G. &. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management,, 16*((1),), 65–74.

Dickinson, G. (2001). Enterprise risk management: its origins and conceptual foundation. *26*, 360-366.

Diefenbach, T. (2009). Are case studies more than sophisticated story telling? Methodological problems of case studies mainly based on semi-structured interviews. *43*(6), 875-894.

Drost, E. A. (2011). Validity and Reliability in Social Science Research. *Education Research and Perspectives, 38*(1), 105-123.

Ellul, A. a. (2013). *Stronger Risk Controls , Lower Risk : Evidence from U . S . Bank Holding Companies,"* (Vol. XVIII).

Emblemsvåg, J. &. (2002). Strategic risk analysis: a field version. *Management Decision, 40*(9), 842 852.

European Central Bank (ECB) Supervision, D. O. (2024, February 20). *https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240220_3~24*

3251dfe9.en.html#:~:text=The%20Act%20lays%20down%20requirements%20for%20ICT%20risk,and%20the%20sound%20management%20of%20ICT%20third-party%20risk. Retrieved January 22, 2025, from https://www.bankingsupervision.europa.eu/: https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240220_3~243251dfe9.en.html#:~:text=The%20Act%20lays%20down%20requirements%20for%20ICT%20risk,and%20the%20sound%20management%20of%20ICT%20third-party%20risk.

European Central Bank, B. S. (2024, November 13). *https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2024/html/ssm.nl241113_4.en.html*. Retrieved October 13, 2024, from https://www.bankingsupervision.europa.eu: https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2024/html/ssm.nl241113_4.en.html

Fischer. (2011). *Risk Analaysis perspectives of Risk Taking and the Media* (Vol. 31). John Wiley & Sons, Inc.

Flanagan, R. &. (1993). *Risk management and construction,.* London: Blackwell Scientific Publications,.

Flick, U. (2002). *An Introduction to Qualitative Research (2nd ed.).* . London: Sage Publications.

Frame, J. D. (2003). *Managing risk in organizations: A guide for managers,.* NY, US.: Jossey-Bass,.

Fraser, J. S. (2014). Implementing Enterprise Risk Management: Case Studies and Best Practices. *John Wiley & Sons.*

Gallagher, J. (2005). *Managing IT Risk: A Practical Guide for Managers..* Wiley.

GAO. (1999). GAO/AIMD-00-33 Information Security Risk Assessment. In GAO, *Executive Guide on Information Security Management. United States General Accounting Office,.* Washington, D.C.: United States General Accounting Office.

Gerrard, D. (2017). "The Role of IT Risk Management in Financial Institutions". *Financial Systems Review.*

Ghazouani, M. F. (2014). Information security risk assessment: a practical approach with a mathematical formulation of risk. *International Journal of Computer Applications, 103(8),* 36-42.

Gottfried, I. (1989). When disaster strikes. *Journal of Information Systems Management*, 86-89.

Haneef, M. A. (2012, April). Impact of Risk Management on Non- Performing Loans and Profitability of Banking Sector of Pakistan. *International Journal of Business and Social Science, Vol. 3 No. 7;* , 307-315.

Haseeb, M. X. (2011). HAZARD RISK ANALYSIS AND MANAGEMENT IN CONSTRUCTION SECTOR OF PAKISTAN. *International Journal of Economics and Research,, 2*(4), 35-42.

Hirschhein, S. &. (2003). An extended platform logic perspective of IT governance: managing perceptions and activities of IT. *The Journal of Strategic Information Systems*, 129-166.

Hora, M. &. (2013). Learning from others'misfortune: factors influencing knowledge acquisition to reduce operational risk. *J. Oper. Manag,, 31*(1), 52–61.

Horcher, K. (2005). Essentials of financial risk management. In K. A. Horcher, *Essentials of Financial Risk Management* (pp. 149-177). John Wiley & Sons.

Hsieh, H. &. (2017). Information technology risk management frameworks: A comparative analysis. *Journal of Information Systems, 31*(2), 89-105.

Huang, C. H. (2015). "Integrating Enterprise Risk Management and IT Systems: A Holistic Approach". *Risk Management Journal.*

Hubbard, D. W. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It* (2nd Edition ed.). John Wiley and Sons.

Hull, J. C. (2012). *Risk Management and Financial Institutions.* John Wiley & Sons,.

IFACI, P. &. (2005). *Le management des risques de l'entreprise Cadre de Référence.* echniques d'application. Editions d'Organisation.

IMF, T. F. (2020, Jan 28). *https://www.elibrary.imf.org/view/journals/002/2020/029/article-A000-en.xml*. Retrieved February 28, 2024, from https://www.elibrary.imf.org: https://www.elibrary.imf.org/view/journals/002/2020/029/article-A000-en.xml

INSA. (2023). *INSA Report.* Addis Ababa: Information Network Security Administration.

ISACA ,. (2020b). *https://www.isaca.org/resources/risk-it-practitioner-guide-2nd-edition*. Retrieved 12 22, 2023, from https://www.isaca.org: https://www.isaca.org/resources/risk-it-practitioner-guide-2nd-edition

ISACA. (2009). *The Risk IT Framework,.* ISACA.

ISACA,. (2019). COBIT 2019 Framework: Governance and Management of Enterprise IT. *ISACA Publications.*

ISACA. (2016b,). *Risk IT framework,.* ISACA.

ISACA., I. (2020a). *Risk IT Framework, 2nd Edition.* Schaumburg, Illinois, USA: ISACA.

ISO. (2018). Risk Management—Guidelines. *International Organization for Standardization.*

ISO. (2009 b). ISO Guide 73:2009 - Risk management . *Vocabulary*.

ISO/IEC 27005, I. (2011). *Information technology – Security techniques – Information security risk management.* INTERNATIONALSTANDARD.

ISO/IEC, 2. (2013). *Information technology – Security techniques – Information security management systems – Requirements.* International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Jordan, E. (2005). An integrated it risk model. *PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS (PACIS* (pp. 632-644). Sydney, Australia: Association for Information Systems.

K.Yin, R. (2018). *Case study research and applications: Design and methods* (6th ed. ed.). Thousand Oaks, CA:: SAGE Publications.

Kaplan & Garrick. ((1981)). On the quantitative definition of risk. *Risk Analysis,, 1*(1), 11-27.

Kaplan, R. S. (2012). Managing risks: A new framework. *Harvard Business Review,, 90*(6), 48-60.

Kaselowski, E. (2008). Mitigating risk through effective information technology operations in local governments: Towards a best practice. *Journal of Management Information Systems, 36*(1), 120–157.

Kaspersky, E. A. (2023, May 7). *https://www.kaspersky.com/blog/secure-futures-magazine/ethiopia-digital-transformation-strategy/39783/*. Retrieved September 17, 2024, from https://www.kaspersky.com/blog/secure-futures-magazine: https://www.kaspersky.com/blog/secure-futures-magazine/ethiopia-digital-transformation-strategy/39783/

Khatibi, M. e. (2020). "Cybersecurity Risk Management in Financial Institutions". . *International Journal of Cybersecurity.*

Kiran, K. (2013). A Comparative Analysis on Risk Assessment Information Security Models. *International Journal of Computer Applications,* 0975 – 8887.

Knight, F. H. (2006). *Risk, Uncertainty and Profit.* Cosimo.

Kouns, J. &. (2011). nformation technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams. *John Wiley & Sons.*

KPMG. (2014). *Enterprise risk management, from theory to practice.* Retrieved July 12 , 2018, from KPMG: https://www.in.kpmg.com/SecureData/aci/Files/KPMG_ERM_Theory_Practices.pdf

Krippendorff, .. a. (2008). *The Content Analysis Reader.* Losangles: SAGE Publications, Inc;.

Kumsuprom, S. (2010). Structured approach to organisational ICT risk management.

Kutsch E., T. R. (2016). Bridging the Risk Gap : The Failure of Risk Management in Information Systems Projects.

Le Roux, H. (2009). Conceptual enterprise risk management implementation enterprise model and proposed management. *North-West University (South Africa), Vaal Triangle Campus*, 90-180.

Lei, Y. (2011). Minimizing the Cost of Risk with Simulation Optimization Technique. *Risk Management and Insurance Review,, 14*(1), 121-144.

Liang, L. R. (2013). The state of the art of risk assessment and management for information systems. *9th International Conference on Information Assurance and Security (IAS).*

Longstaff, T. C. (2000). Are We Forgetting the Risks of Information Technology? *Journal of Computer*.

Loosemore, M. R. (2006). Risk Management in Projects. *Oxon: Taylor & Francis.*

Lyons, S. (2015). Enterprise risk management and the five lines of corporate defence. *The Journal of ERM*, 56-81.

Macedo, F. &. (2009). Comparative study of information security risk assessment models. 1-11.

Markus, M. L. (2000). Paradigm shifts—E-business and business/systems integration. *Communications of the Association for Information Systems,*, 1–44.

Markus, M. L. (2000). Paradigm shifts—E-business and business/systems integration. *Communications of the Association for Information Systems,*, 1–44.

Martin, G., B. R., & and Cooper, C. .. (2011). *Corporate Reputation; Managing Opportunities and Threats* (1st Edition ed.). london, England: Ashgate.

May, A. G. (2011, January 19). Systemic risk in banking ecosystems. *Nature, 469*, 351–355.

McConnell, P. (2015). Strategic Risk Management: a trail of two strategies. *Macquarie University Faculty of Business & Economics Research Paper*, 2-29.

McFadzean, E. E. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *https://doi.org/10.1108/14684520710832333, Vol. 31*, pp. 622-660.

McKim, C. (2023). Meaningful Member-Checking: A Structured Approach to Member-Checking. *American Journal of Qualitative Research,, 7*(2), 41-52.

Mcube, U. (2016, May 11-13). A scenario-based ICT risk assessment in local government.

MetLife, U. S. (2010). *MetLife (MET) Historical Annual Reports 2003-2024.* Washington: MetLife, Inc.

Mohammad, A. G.-I. (2014). Establishing effective guidelines to avoid failure and reducing risk in e-business. International Journal of Current Engineering and Technology. *International Journal of Current Engineering and Technology, 4*(1), 28-31.

Moore, D. S. (2005). *Introduction to the Practice of Statistics (5th ed.).* New York, NY: : W.H. Freeman & Company.

NBE ., N. t. (2023-2026, Aughst). *NBE news*. Retrieved February 15, 2024, from https://nbe.gov.et/mandates-of-the-bank/: https://nbe.gov.et/mandates-of-the-bank/

NBE. (2023). *National Bank of Ethiopia*. Retrieved from https://nbe.gov.et/

NBE., B. R. (2010, May). *https://nbe.gov.et/wp-content/uploads/2023/04/Rm-Guideline-revised-1.pdf*. Retrieved september 13, 2024, from https://nbe.gov.et/: https://nbe.gov.et/wp-content/uploads/2023/04/Rm-Guideline-revised-1.pdf

NBE., N. B. (2003). Retrieved 8 13, 2024, from https://nbe.gov.et: https://nbe.gov.et/wp-content/uploads/2023/04/Rm-Guideline-revised-1.pdf

Newman., M. M. (2007). The Qualitative Interview in IS Research: Examining the Craft. *Information and Organization, 17*(1), 2-26.

NIST. (2018). *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy.* Gaithersburg, MD 20899-8930: National Institute of Standards and Technology Special Publication 800-37, Revision 2.

NIST. (2020, DEcember 10). *https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final*. Retrieved november 14, 2024, from https://csrc.nist.gov: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST., S. 8.-3. (2012, 1 7). *https://csrc.nist.gov/pubs/sp/800/30/r1/final*. Retrieved 10 11, 2024, from https://csrc.nist.gov: https://csrc.nist.gov/pubs/sp/800/30/r1/final

Omotayo, F. (2015, 10 4). Knowledge management as an important tool in organisational management. *Library Philosophy and Practice*, 1-23.

Onwuegbuzie, A. J. (2006). *Linking Research Questions to Mixed Methods Data Analysis Procedures 1. The Qualitative Report,*. Florida: NSUWorks.

Opoku, M. (2015, November 2). Information management and organisational performance. *Mediterranean Journal of Social Sciences*. Rome, Rome, Italy.

Padayachee, K. (2016). Risk culture assessment of a financial services organisation. North-West University (South Africa), Vaal Triangle Campus.

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods (3rd ed.)* ((3rd ed.). ed.). Sage Publications.

Peter L. Wright, M. K. (1997). *Strategic Management: Concepts and Cases.* New Jersey: Prentice Hall.

Pironti, J. (2010). Developing an information security and risk management strategy. *ISACA Journal, 2*, 28-35.

Pirzada, K. &. (2013). Effect of New Technology on Firms Business Objectives: A Case Study of Pak-Suzuki Company. *International Journal of Business Administration, 4*(3).

PMI. (2021.). *A Guide to the Project Management Body of Knowledge (PMBOK Guide) (7th ed.).* Project Management Institute.

Policy Studies Institute, E. D. (2024, February 2). *https://psi.org.et/index.php/blog/266-ethiopia-s-digital-finance-sector-overcoming-challenges-and-driving-financial-inclusion*. Retrieved January 23, 2025, from https://psi.org.et/: https://psi.org.et/index.php/blog/266-ethiopia-s-digital-finance-sector-overcoming-challenges-and-driving-financial-inclusion

Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management. .* New York: Oxford University Press.

Purtell, T. (2007). Building a successful information technology risk management program. *54*, 28-33.

R. Mehdizadeh, D. B. (2013). *Civil Engineering and Environmental Systems Dynamic and multi perspective risk management in construction with a special view to temporary structures,*.

Racz, N. W. (2010). Questioning the need for separate IT risk management frameworks. *GI Jahrestagung.*, 245-252.

Radanlie v., a. P. (2018). Future Developments in Cyber Risk Assessment for the Internet of Things. *ELSEVIER*, 14-22.

(1994). Risk Analysis in Project Management. In J. Raftery. London: E & FN Spon, 1994.

Rainer Jr, R. S. (2015). Risk analysis for information technology. Journal of Management Information Systems. *JSTOR, 8*, 129-147.

Ramamoorti, S. & Sridhar, N. (2013). The importance of information integrity. *Internal Auditor, 70*(1), 29-31.

Rick Nason, B. C. (2018). *Essentials of Financial Risk Management: Practical Concepts for the General Managers.* Business Expert Press.

Roberts, A. W. (2012). *Strategic risk management.* New Jersey: Pearson Education.

Robertson, D. (2016). Introduction to Operational Risk. In Managing Operational Risk. In D. Robertson, *Managing Operational Risk.* New York: Palgrave Macmillan.

Robson, C. (2011). *Real World Research: A Resource for Social-Scientists and Practitioner-Researchers.* Oxford:: BlackwellPublishing.

Rot, A. (2009). Enterprise information technology security: Risk management perspective. *Proceedings of the World Congress on Engineering and Computer Science 2009 Vol II.* San Francisco,USA: https://doi.org/10.1007/s10799-005-5880-5.

Ružić-Dimitrijević, N. &. (2009). Information System and Risk Reassessment. *Information System and Risk Reassessment*, 192-207.

sanjaya, C. $. (2015). Pengaruh Penerapan Enterprise Risk Management dan Variabel Kontrol Terhadap Nilai Perusahaan di Sektor Keuangan. *Finesta*, 52-57.

Satish, R. (2017). *Benefits Of Establishing Goals And Objectives For A Business*. Retrieved January 28, 2017, from Knowledge for success: http://knowledge-4-success.com/

Schermann, M. W. (2014). The role of information systems in supporting exploitative and explorative management control activities. *Journal of Management Accounting Research,, 26*(1), 1–27.

Seale, T. (2017). *https://open.uct.ac.za/items/3cebc826-556e-4b01-8a10-553551404c3e*. Retrieved from https://open.uct.ac.za/: https://open.uct.ac.za/items/3cebc826-556e-4b01-8a10-553551404c3e

Seltiz, C. (1976). *Research methods in social relations.* New York:: Holt Rinehart & Winston.

Sharma, S. K. (2009). Information systems security management: A process standardization framework. *ournal of Global Information Technology Management,, 12*(3), 1–26.

Shenglan Ma, W. H.-N. (2018). A Blockchain-Based Risk and Information System Control Framework. *IEEE 16th Intl Conf on Dependable, Autonomic and Secure ComputingComputing and Cyber Science and Technology Congress.* IEEE.

Shukla, N. &. (2012). A comparative study on information security risk analysis practices. *IJCA Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies*, 28-33.

Sibanda, M. (2024, Jul 16). *https://itweb.africa/content/JN1gP7OABxOqjL6m*. Retrieved september 13, 2024, from https://itweb.africa/: https://itweb.africa/content/JN1gP7OABxOqjL6m

Siponen, M. &. (2009). Information security management standards: Problems and solutions. Information & Management,. *journal Information & Management., 46*(5), 267-270.

Snelbecker, G. E. (1990). Investors' risk tolerance and return aspirations, and financial advisors' interpretations: A conceptual model and exploratory data. *The Journal of Behavioral Economics,*, 377–393.

Stoneburner, G. G. (2002). *Risk Management Guide for Information Technology Systems.* National Institute of Standards and Technology.

Streif. (2013). Information technology risk management. In Strategic Security Management. *IJIERT*, 133-157.

Suroso, J. S. (2017). Development of IT Risk Management Framework Using COBIT 4.1, Implementation In IT Governance For Support Business Strategy. *CM International Conference Proceeding Series. Part F130654,*, (pp. 92-96.).

Svatá, a. M. (2009). S / IT Risk Management In Banking Industry,. *Acta Oeconomica Pragensia,*, *19*(3), 42–60.

Swanepoel, E. &. (2015). A structured approach to risk identification for projects in a research environment. *Portland International Conference on Management of Engineering and Technology (PICMET)*, 1719-1725.

Tadesse, B. &. (2024). Electronic-Banking in Ethiopia: Practices, Opportunities and Challenges. *Innovations,*, *15*(2), 1235-1245.

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable.* . New york: Random House.

Taylor, H. E. (2012). Information technology project risk management: Bridging the gap between research and practice. *Journal of Information Technology* , 17-34.

Teilans, A. R. (2011). Functional modelling of IT risks assessment support system. *Economics & Management, 16*, 1061-1068.

Teymouri, M. &. (2011). The impact of information technology on risk management. *Procedia Computer Science 3*, 1602–1608.

The Institute of Risk Management. (2012). *Risk culture.* London: Palgrave Macmillan UK.

Ukwandu, E. A. (2013). The Effects of Information Technology on Global Economy. *The Social Sciences, 8*, 606-609.

Van Grembergen, W. &. (2009). *Enterprise Governance of IT.* springer.

Vidalis, S. (2004). A critical discussion of risk and threat analysis methods and methodologies. *IFIP INTERNATIONAL INFORMATION sECURITY CONFERENCE Technical report CS-04-03. School of Computing, University of Glamorgan. 354*, pp. 259–270. Heidelberg,Berlin: Springer.

Viscelli, T. B. (2016). Research insights about risk governance: Implications from a review of ERM research. *SAGE Open, 6*(4).

Von Solms, S. &. (2009). Information security governance. *Springer*.

Vorecol . (2024, August 28,). *https://vorecol.com/blogs/blog-enhancing-employee-training-through-competency-assessments-37601?utm_source=chatgpt.com*. Retrieved november 19, 2024, from https://vorecol.com/blogs: https://vorecol.com/blogs/blog-enhancing-employee-training-through-competency-assessments-37601?utm_source=chatgpt.com

Walke, R. C. (2011). An approach to risk quantification in construction projects. *International Journal of Engineering Science and Technology, 3*(9), 6846-6855.

Ward, J. &. (2002). *Strategic Planning for Information Systems.* New York,: J. Wiley.

Westerman, G. (2007). IT risk as a language for alignment: Using leadership profiles to optimize value. *MIT Sloan CISR Research Briefing*, 1-4.

Wiesche, M. J. (2013). Grounded theory methodology in information systems research. *MIS Quarterly*, , 735–757.

Wiesche, M. J. (2013). Grounded theory methodology in information systems research. *MIS Quarterly*,, *37*(3), 735–757.

Willcocks, L. L. (1999, September). Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA. *Journal of Strategic Information Systems, 8*(3), 285-314.

World Bank,. (2024, March 15). *https://blogs.worldbank.org/en/nasikiliza/leveraging-e-payments-financial-inclusion-ethiopia-afe-0324*. Retrieved January 23, 2025, from https://blogs.worldbank.org/: https://blogs.worldbank.org/en/nasikiliza/leveraging-e-payments-financial-inclusion-ethiopia-afe-0324

world Bank, W. B. (2024, December 19). *https://www.worldbank.org/en/news/press-release/2024/12/19/world-bank-supports-afe-ethiopias-efforts-to-unleash-the-potential-of-its-financial-sector#:~:text=WASHINGTON%2C%20December%2019%2C%202024%20%E2%80%93%20The%20World%20Bank,%28IDA%29%2A%20for%20the*. Retrieved January 19, 2025, from https://www.worldbank.org/: https://www.worldbank.org/en/news/press-release/2024/12/19/world-bank-supports-afe-ethiopias-efforts-to-unleash-the-potential-of-its-financial-sector#:~:text=WASHINGTON%2C%20December%2019%2C%202024%20%E2%80%93%20The%20World%20Bank,%28IDA%29%2A%20for%20the

World Bank., W. D. (2016, January 14). *https://www.worldbank.org/en/publication/wdr2016*. Retrieved September 2, 2024, from https://www.worldbank.org/: https://www.worldbank.org/en/publication/wdr2016

World Economic Foroum, T. F. (2020, October 20). *https://www.weforum.org/publications/the-future-of-jobs-report-2020/*. Retrieved November 12, 2024, from https://www.weforum.org: https://www.weforum.org/publications/the-future-of-jobs-report-2020/

World Economic Forum's. (2021, March 23). *https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/?utm_source=chatgpt.com*. Retrieved January 21, 2024, from https://www.weforum.org/: https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/?utm_source=chatgpt.com

Y. Liu, L. W. (2016). *Experimental and numerical studies on the effect of inlet pressure on cavitating flows in rotor pumps,* (Vol. 4). Arabian Journal for Science and Engineering.

Yibeltal, K. (2024, March 18). *https://www.bbc.com/news/world-68599027*. Retrieved september 13, 2024, from https://www.bbc.com: https://www.bbc.com/news/world-68599027

Young L, I. (2020, june 25). *https://www.isaca.org/about-us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology*. Retrieved 10 5, 2024, from https://www.isaca.org/: https://www.isaca.org/about-us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology

Zhang, Y. (2009). A Study on Risk Cost Management. *International Journal of Business and Management, 4*(5), 145-148.

Zuckerman, M. (1994). *America's silent revolution.* U.S. News and World Report.

Appendix A: Semi-Structured Interview Guide for ISMD and IARMD

The questions are structured around the three domains of the Risk IT Framework: Risk Governance, Risk Evaluation, and Risk Response. Your views will help shape a more effective and tailored IT risk management framework for the Bank.

1. Could you please tell me your current job title or role within the Bank?
2. How long have you been serving in this position, and have you held any related roles in the past at the Bank?
3. Can you briefly describe your main responsibilities in this role, especially as they relate to IT systems or risk management?

Section I: General Context Questions

1. From your perspective, what are the most pressing IS-related challenges currently facing the Bank? Could you share an example of how one of these challenges has affected your department or daily work?
2. Can you walk me through how IS risk is currently handled within your area or unit? What kind of involvement do you and your team have in this process?

Section II: Risk Governance

3. How would you describe the way different departments at the Bank come to a shared understanding of IT risks? Are there regular meetings or specific ways this is encouraged?
4. Have you experienced situations where IT and business teams saw risks differently? If so, how was that gap addressed?
5. Can you explain how IT risk fits into the Bank's overall risk management strategy? In your role, how do you see this connection play out?
6. What challenges have you seen in aligning IT risk with the Bank's broader goals and regulatory demands? How does the Bank try to overcome those challenges?
7. Have you been involved in business decisions like selecting a vendor or launching a system where IT risk data influenced the outcome? How was the information used?
8. Could you describe a time when awareness of an IT risk changed how a major decision was made at the Bank? What happened, and what was your role in it?

Section III: Risk Evaluation

9. In your experience, how does the Bank gather and track data about IT incidents or risks like system downtime, threats, or vulnerabilities?
10. Who usually takes the lead in collecting and verifying this data? How confident are you in the accuracy and timeliness of this information?
11. Are you aware of specific tools or approaches the Bank uses to assess IT risk such as key risk indicators or risk scenarios? Have you used or seen these applied in your area?
12. How does the Bank stay ahead of new or emerging IT risks like those coming from fintech or changes in cyber threats? Are there formal ways this is done?
13. From your experience, how often is the Bank's IT risk profile updated to reflect changing threats? Is this something you or your team interact with?
14. Who usually reviews the risk profile at a higher level? Do you know how this document influences strategic or operational decisions?

Section IV: Risk Response

15. When an IT risk is identified like a cyber-threat or system outage how is that information communicated to you or your team? Are there clear channels and formats for doing this?
16. In your view, how well are IT risks explained to people who don't have a technical background? Are there efforts to make this communication more accessible?
17. Based on your experience, which types of risk response strategies such as mitigating, accepting, or transferring risk are most commonly applied at the Bank?
18. When big IT risk decisions need to be made, who is typically at the table? Have you ever been involved in one of these discussions?
19. Can you describe what usually happens when a serious IT incident occurs, such as a cyberattack or major system failure? What's your role in the response?
20. Could you share a recent example of an IT-related issue the Bank faced? What went well in how it was handled, and what lessons were learned?

Appendix B: Interview Guide for Business Unit Participants

1. Could you please tell me your current job title or role within the Bank?
2. How long have you been serving in this position, and have you held any related roles in the past at the Bank?
3. Can you briefly describe your main responsibilities in this role, especially as they relate to IT systems or risk management?

Based on the Risk IT Framework

1. From your perspective, what are the most significant information system challenges the Bank currently faces, and how have these challenges affected your department's day-to-day operations?
2. Based on your experience, how is information system risk management currently handled within the Bank, and what role do you and your team play in that process?
3. In your view, how clearly has the Bank communicated its information system risk appetite and tolerance levels to business units like yours? How do these guidelines influence your department's strategic or operational decisions?
4. Are you aware of any governance structures or committees that oversee information system risk management? If so, how do you see their role impacting your unit's responsibilities or input into information system related decisions?
5. How information system risk is considered within broader business risk discussions in your unit? In what ways do you see information system risk being integrated into the Bank's overall Enterprise Risk Management (ERM) framework?
6. Can you describe a time when your department used information system risk-related information (such as audit findings, incident reports, or risk assessments) to support a business decision, like choosing a vendor or adjusting an operational process?
7. In your experience, how well does the Bank monitor and respond to emerging technology risks such as those related to digital transformation or evolving cyber threats?
8. How confident are you that the Bank information system risk profile reflects current realities, such as the growth of fintech in Ethiopia or the increasing complexity of cyber security threats? Why or why not?
9. When an information system risk like a potential system failure or security vulnerability is identified, how is this typically communicated to you or your department? Do you feel that communication is timely and actionable?

10. As someone in a non-technical role, how well do you understand the information system risks communicated to you? Are there ways this communication could be improved to support better decisions on your side?
11. From your experience, who usually takes part in making key decisions around managing serious information system risks? Do you feel your team's input is considered in those decisions?
12. Can you recall a specific incident where your unit had to respond to an information system related issue? What was your role, and what aspects of the response worked well or didn't?

Appendix C: Expert Evaluation Responses

Table: Expert Evaluation Responses to the Proposed IT Risk Management Framework

Evaluation Dimension	Expert Feedback Summary	Key Expert Comments	Improvement Suggestions
Relevance			
Comprehensiveness			
Practicality			
Alignment with Best Practices			

Appendix D: Observation Checklist Based on the ISACA Risk IT Framework (2009)

Purpose: To assess the presence and effectiveness of IT risk management practices in line with the Risk IT Framework.

Domain	Observation Item	Yes / No / Partial	Remarks / Notes
Risk Governance	Is there a formally approved IT risk management policy aligned with strategic objectives?		
	Is IT risk integrated into the enterprise risk management (ERM) framework?		
	Are IT risk roles and responsibilities clearly defined and assigned?		
	Is there oversight of IT risk by senior management or the board?		
	Is the organization's IT risk appetite and tolerance level documented?		
	Are IT risk policies reviewed and updated regularly?		
Risk Evaluation	Is there a structured methodology for identifying IT risks (e.g., threat,		

	vulnerability, asset analysis)?		
	Are risks assessed based on likelihood, impact, and business alignment?		
	Are risk scenarios developed for high-risk areas such as cybersecurity or third-party services?		
	Is there a centralized IT risk register that is regularly maintained?		
	Are both business and IT units involved in the risk assessment process?		
	Are evaluation results reported to decision-makers for informed action?		
Risk Response	Are risk treatment options (avoid, reduce, transfer, accept) clearly defined and applied?		
	Are risk mitigation plans documented, resourced, and implemented?		
	Is there a mechanism for tracking the effectiveness of risk response actions?		
	Are IT risk responses integrated with incident response and business continuity planning?		
	Are lessons learned or audit findings used to improve future risk response activities?		