 

**BANK OF TANZANIA**

**Proposal: Assessment of Cybersecurity Controls in Mobile Financial Services in Tanzania**

Eng. Bernard Kambanga, Dr. Romwald Lihakanga (PhD), and Emmanuel Kajange

March 2025

**LIST OF ACRONYMS**

**Acronym Description**

AU African Union

BOT Bank of Tanzania

CBK Central Bank of Kenya

CERT Computer Emergency Response Teams

EAC East African Community

EACC East African Centre for Cybersecurity

EADB East African Development Bank

EACO East African Communications Organization

ENISA European Union Agency for Cybersecurity

GDPR General Data Protection Regulation

IJFMR International Journal for Multidisciplinary Research

MFS Mobile Financial Services

MNO Mobile Money Operators

MFA Multi-Factor Authentication

NIST National Institute of Standards and Technology

PMT Protection Motivation Theory

PPPs Public-Private Partnerships

RBV Resource-Based View Theory

SADC Southern African Development Community

TCC Tanzania Cybersecurity Centre

TCRA Tanzania Communications Regulatory Authority

TOE Technology-Organization-Environment

Table of Contents

[1. Introduction 4](#_Toc201609248)

[1.1. Statement of the problem 4](#_Toc201609249)

[1.2. Research Objectives 4](#_Toc201609250)

[1.3. Research Questions 4](#_Toc201609251)

[1.4. Research Significance 5](#_Toc201609252)

[2. Literature Review 5](#_Toc201609257)

[2.1. Theoretical Framework 5](#_Toc201609258)

[2.2. Empirical Framework 6](#_Toc201609259)

[2.3. Identified Gap and Research Justification 8](#_Toc201609260)

[2.4. Conceptual Framework 9](#_Toc201609261)

[2.5. Conceptual framework Diagram Description 10](#_Toc201609262)

[3. RESEARCH METHODOLOGY 10](#_Toc201609263)

[4. Research activities, duration, work plan and budget estimate 14](#_Toc201609264)

[2.6. References (APA 7th Edition Format) 18](#_Toc201609265)

[2.7. Appendices 19](#_Toc201609266)

# Introduction

Mobile Financial Services (MFS) have transformed Tanzania's financial landscape, significantly enhancing financial inclusion by providing essential financial services such as fund transfers, bill payments, and micro-loans, particularly beneficial to the unbanked and underbanked populations. As these services expand, cybersecurity threats have concurrently grown, including sophisticated fraud, phishing attacks, unauthorized access, and SIM-swap fraud. These threats capitalize on security vulnerabilities within mobile platforms, undermining consumer trust and jeopardizing financial stability. Data from the Tanzania Communications Regulatory Authority (TCRA, 2024) and the Bank of Tanzania (BoT, 2023) highlight a marked rise in cybersecurity incidents, emphasizing the urgent need for robust cybersecurity controls.

## Statement of the problem

Despite established regulatory frameworks, including the Cybercrimes Act (2015), Personal Data Protection Act (2022), and guidelines by regulatory bodies like BoT and TCRA, Tanzania continues to experience escalating cybersecurity incidents. TCRA reports indicate significant increases in fraudulent incidents, notably a 52 percent rise involving the Airtel network, alongside considerable growth in fraud incidents affecting Halotel and TTCL. Moreover, high-profile cases, such as the Leo Beneath London (LBL, 2025) online lending fraud, expose critical deficiencies in the current cybersecurity infrastructure and regulatory oversight, underscoring gaps in fraud detection, timely intervention, and consumer protection mechanisms. Research by Mwakalinga and Mushi (2020) and Omary and Kyaruzi (2022) corroborates persistent security weaknesses that compromise user trust and service stability, highlighting the critical need for a comprehensive evaluation of existing cybersecurity controls to ensure effective risk management and consumer protection.

## Research Objectives

The primary objective of this research is to evaluate the effectiveness of cybersecurity controls implemented within Tanzania’s mobile financial services sector. Specifically, the research aims to:

1. Identifying Implemented Cybersecurity Controls
2. Evaluating Adequacy of Implemented Cybersecurity Controls
3. Assessing Performance of Implemented Cybersecurity Controls

## Research Questions

To guide this study, the following research questions have been formulated:

1. What cybersecurity controls have been implemented by Mobile Financial Service providers in Tanzania?
2. To what extent are the implemented cybersecurity controls adequate in addressing the identified risks and complying with relevant standards and regulations?
3. How effective are the implemented cybersecurity controls in preventing, detecting, and responding to cyber threats within Mobile Financial Services?

## Research Significance

This study will have the following significance:

## Strengthening the cybersecurity posture of Tanzania's financial sector.

## Supporting evidence-based policymaking.

## Enhancing consumer protection, digital trust, and resilience of MFS platforms.

## Aligning local cybersecurity practices with international standards and national regulatory frameworks.

# Literature Review

This section provides an overview of existing research and findings related to assessing Cybersecurity controls in the context of mobile financial services, focusing on global, regional, and local perspectives.

## Theoretical Framework

Understanding cybersecurity control effectiveness in mobile financial services (MFS) requires multi-dimensional theoretical grounding. This study employs four key theories namely: Technology-Organization-Environment (TOE) Framework, Protection Motivation Theory (PMT), Deterrence Theory, and Resource-Based View (RBV). Each is examined below with its strengths, limitations, and relevance to the research that provide a solid foundation for understanding user adoption, regulatory enforcement, and the role of institutional policies.

* + 1. **Technology-Organization-Environment (TOE) Framework**

The TOE framework, proposed by Tornatzky and Fleischer (1990), suggests that technological innovation adoption within organizations is influenced by three main contexts: technological context (availability and characteristics of cybersecurity technologies), organizational context (structure, size, and resources of the mobile financial service providers), and environmental context (regulatory environment, industry norms, and competitive pressures).

In the context of cybersecurity in mobile financial services, the technological dimension in-volves analyzing available cybersecurity technologies, their compatibility, complexity, and rela-tive advantages. The organizational dimension examines the internal resources of MFS pro-viders, including financial capacity, skilled personnel, and management commitment to cyber-security initiatives. The environmental dimension evaluates external pressures, such as regulatory mandates by institutions like the Bank of Tanzania (BoT) and competitive dynamics among mobile service providers.

Applying the TOE framework allows for a holistic assessment of how various internal and ex-ternal factors collectively influence the adoption and effectiveness of cybersecurity measures. This framework will guide the identification of variables related to technology adoption, organizational readiness, and environmental pressures in the data collection process.

* + 1. **Protection Motivation Theory (PMT)**

Protection Motivation Theory (PMT), developed by Rogers (1983), focuses on individual psychological reactions to perceived threats. It highlights two key cognitive processes influencing behavior: threat appraisal and coping appraisal.

Threat appraisal assesses how individuals perceive the severity of cybersecurity threats and their vulnerability to these threats, while coping appraisal evaluates their belief in the efficacy of protective measures and their self-efficacy to implement such measures effectively. In Tanzania’s MFS sector, PMT explains why some consumers actively engage in protective behaviors, such as using multi-factor authentication and maintaining strong passwords, while others do not, despite being aware of threats.

Understanding these behavioral dynamics can significantly inform targeted consumer education programs and enhance overall cybersecurity practices. This theory will help identify variables related to user behavior and motivation, which can be assessed during data collection. In this research, PMT complements the TOE framework by providing insights into how behavioral perceptions affect cybersecurity adherence among employees and users within the MFS environment.

* + 1. **Deterrence Theory**

Deterrence Theory, introduced by Becker (1968), posits that individuals are discouraged from committing undesirable acts when they perceive a high likelihood of detection and punishment. Applied to cybersecurity, the theory suggests that strong regulatory enforcement, such as stiff penalties under Tanzania’s Cybercrimes Act (2015) and Data Protection Act (2022), can deter malicious actions or negligence among MFS stakeholders. The strength of Deterrence Theory is its clear policy relevance—highlighting the role of legal frameworks in influencing organizational behavior and compliance. However, its assumption that individuals always act rationally may not hold in cases involving carelessness or low awareness. Nonetheless, it is highly relevant in this study for evaluating how effectively regulatory structures contribute to reducing cybersecurity incidents and encouraging best practices across the MFS sector.

* + 1. **Resource-Based View (RBV) Theory**

The Resource-Based View (RBV) Theory, articulated by Barney in 1991, argues that sustainable competitive advantage arises from an organization’s ability to acquire and manage strategic resources that are valuable, rare, inimitable, and non-substitutable. In the realm of cybersecurity, such resources include advanced technical systems, skilled personnel, threat intelligence, and robust governance frameworks. RBV’s strength lies in its focus on internal capability development, allowing differentiation among MFS providers based on how well they allocate and leverage resources to manage cybersecurity threats. Its limitation is the narrow attention to external factors like regulation and environmental dynamics. Despite this, RBV is highly applicable in this research to assess institutional differences in cybersecurity capacity and how those differences influence control performance across providers.

Integrating these four theoretical frameworks (TOE, PMT, Deterrence Theory, and RBV) offers a comprehensive analytical foundation for understanding multiple dimensions of cybersecurity management in Tanzania's mobile financial services sector. This integrative theoretical perspective enables an in-depth exploration of organizational, regulatory, technological, and behavioral dimensions influencing cybersecurity effectiveness, providing robust guidance for both empirical investigation and practical policy recommendations.

## Empirical Framework

The empirical evidence from various studies offers critical insights into the state of cybersecurity controls in mobile financial services. This empirical framework systematically reviews these studies, focusing explicitly on identified cybersecurity threats, the effectiveness of implemented control measures, and the critical gaps that this research seeks to address.

Globally, cybersecurity in digital financial services has received significant attention. The GSMA Mobile Telecommunications Security Landscape report (2022) highlights emerging threats, emphasizing the increasing sophistication of social engineering attacks targeting users' psychological vulnerabilities. Similarly, the Verizon Data Breach Investigations Report (2023) underscores the prevalence of phishing, malware, and ransomware as predominant cybersecurity threats in digital transactions. These studies stress the importance of robust technical measures, such as multi-factor authentication (MFA), encryption, and user-awareness training programs, as critical components of cybersecurity strategies.

Moreover, Abbinante and Valentini (2023) analyzed cybersecurity incidents in online banking, confirming the necessity of proactive threat detection systems and user education to counter evolving cyber threats. These findings indicate a need for comprehensive approaches that incorporate both technical and behavioral strategies.

In Africa, cybersecurity issues are amplified by infrastructure inadequacies, inconsistent regulatory frameworks, and low user awareness. The IMF’s Global Financial Stability Report (2024) explicitly identifies Africa as vulnerable, citing increased mobile financial fraud largely due to weak regulatory oversight and inadequate enforcement mechanisms. The African Union's Malabo Convention (2014), although intended to harmonize cybersecurity policies across member states, has encountered implementation challenges, further complicating effective cybersecurity governance across the continent.

McKinsey and Company (2022) highlights the potential of Public-Private Partnerships (PPPs) to enhance cybersecurity infrastructure and resilience in Africa, suggesting that collaboration between government and private sector actors is vital for mitigating cybersecurity threats. INTERPOL’s African Cyber Threat Assessment Report (2020) similarly notes that digital financial fraud is increasingly prevalent, emphasizing the urgency of strengthening institutional frameworks and regulatory enforcement.

Within the East African Community, nations reveal specific cybersecurity threats affecting mobile financial services. Omondi (2020) extensively studied the surge in phishing and SIM-swap fraud targeting M-Pesa users in Kenya, particularly intensified during the COVID-19 pandemic. The study identified significant gaps in consumer protection mechanisms, regulatory oversight, and cybersecurity awareness among users.

The East African Centre for Cybersecurity (EACC, 2021) also reported significant disparities in cybersecurity readiness among EAC states, underscoring the necessity for regional coordination and standardized cybersecurity frameworks. Further, the East African Development Bank (EADB, 2022) documented the increased prevalence of mobile financial fraud across the region, highlighting inadequate fraud detection systems and enforcement inconsistencies as primary challenges.

Empirical studies specifically focused on Tanzania provide a deeper understanding of local cybersecurity threats and the effectiveness of existing controls. Mwakalinga and Mushi (2020) identified significant vulnerabilities within Tanzania’s mobile money ecosystem, notably limited consumer cybersecurity awareness and insufficient implementation of technical security controls. Their study emphasized the urgent need for more comprehensive user education and substantial cybersecurity infrastructure among service providers.

Omary and Kyaruzi (2022) evaluated Tanzania’s national cybersecurity policy implementation in the financial sector, highlighting significant enforcement gaps and inadequate compliance among financial service providers. Their research recommended continuous policy updates, stricter enforcement, and increased institutional capacity building to combat emerging cybersecurity threats effectively. Furthermore, recent reports from the Tanzania Cybersecurity Centre (TCC, 2022) and the Bank of Tanzania (BoT, 2023) underscore the rise of SIM-swap fraud and phishing attacks, reflecting ongoing challenges in consumer protection and fraud detection effectiveness.

The most appropriate theoretical framework and approach should be capable of addressing organizational, technological, and environmental factors. Technology-Organization-Environment (TOE) Framework found to be the Best-Fit Theoretical Framework and is the most applicable since it combines three key elements which are technology, organization and environmental as well.

* Studies like Omary and Kyaruzi (2022) that evaluate policy and implementation are conceptually aligned with TOE's structure as it inherently involves technology (cybersecurity systems), organization (policy, training, readiness), and environment (regulation, cyber threats, user behavior).
* Studies by McKinsey (2022) and INTERPOL (2020): showing how environmental and organizational aspects drive technological outcomes. These reports emphasize environmental and organizational collaboration (PPPs).
* The mentioned studies accommodates descriptive data analysis, allowing for exploratory insights into how cybersecurity controls are implemented and influenced.
* Protection Motivation Theory (PMT) is supportive but less central since it focuses on individual behavior and motivation in response to perceived threats (SIM card fraud or phishing attacks). It may serve as a complementary lens within the TOE’s organizational component (staff awareness and behavior).

## Identified Gap and Research Justification

The reviewed literature shows that:

* Globally, robust controls require a blend of technical, behavioral, and regulatory measures.
* Regionally, Africa struggles with institutional fragmentation, capacity issues, and weak enforcement.
* Locally, there is inadequate data on the effectiveness and adequacy of controls implemented by MFS providers in Tanzania.

Gap Statement:

There is limited empirical research assessing the performance and adequacy of cybersecurity controls within Tanzania’s MFS ecosystem using a holistic, multi-theory framework that integrates technological, organizational, behavioral, and regulatory dimensions.

This gap justifies:

* Using TOE to structure variable identification (technology readiness, organizational capacity, regulatory influence).
* Integrating PMT, RBV, and Deterrence Theory to model user behavior, institutional resources, and compliance environments.
* Developing variables aligned to these dimensions for surveys, interviews, and document analysis.

## Conceptual Framework

The conceptual framework integrates key theoretical foundations and empirical findings to provide a structured understanding of how cybersecurity threats, mitigation measures, institutional regulations, and consumer behavior interact to influence cybersecurity effectiveness in Tanzania’s MFS sector. The framework vvisually represents the logical flow and relationship between the **inputs, processes (activities), and outputs** of research focused on cybersecurity controls in the Mobile Financial Services sector.

* 1. **Inputs (Independent Variables)**
* Identification of Implemented Cybersecurity Controls which involves cataloging and documenting the current cybersecurity measures deployed by service providers.
* Evaluation of Adequacy of Implemented Cybersecurity Controls by assesing whether these controls sufficiently cover the risks and comply with standards.
* Assessment of Performance of Implemented Cybersecurity Controls by examining how effectively the controls operate in practice, including detection, prevention, and response capabilities.
  1. **Activities/Processes (Mediating Variables)**

These represent the **research and analytical processes** applied to the inputs to achieve the study objectives, it includes:

* Data collection (surveys, interviews, document review) to identify controls.
* Gap analysis comparing current controls against standards.
* Performance measurement using incident reports, control test results, and monitoring data.
* Formulating practical recommendations through expert consultation and best practices review.
  1. **Output (Dependent Variable)**

The primary output of this framework is the “**Effectiveness of Cybersecurity Controls”. It** reflects the overall security posture of the Mobile Financial Services sector after considering the identification, evaluation and assessment. Effectiveness here means the ability of MFS providers’ cybersecurity measures to protect against, detect, and respond to threats effectively.

## Conceptual framework Diagram Description

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Inputs**   * Identification of Implemented Cybersecurity Controls * Evaluation of Adequacy of Implemented Controls * Assessment of Performance of Implemented Controls | → | **Activities/processes**   * Data Collection (surveys, interviews, document reviews) * Gap Analysis and Compliance Check * Performance Testing and Monitoring | → | **Output**   * Effectiveness of Cybersecurity Controls * Real-world performance |

**Source: Author**

From the diagram above, the framework helps to guide the research by linking the research objectives (inputs) to the research activities and finally to the expected outcome (output). The study starts with **identifying controls (Input);** Then, it evaluates how adequate and how well those **controls perform (Input)**; These inputs feed into research activities which are the data analysis, evaluation, assessment, and recommendation formulation (Processes), and the **output variable, “Effectiveness of Cybersecurity Controls**,” which is the success of the entire process.

# RESEARCH METHODOLOGY

* 1. **Research Design**

This study adopts a descriptive research design aimed at systematically exploring and documenting the current state of cybersecurity controls within Tanzania’s Mobile Financial Services (MFS) sector. The design focuses on describing existing practices, stakeholder perceptions, institutional readiness, regulatory oversight, and the overall effectiveness of implemented cybersecurity measures. The approach is most appropriate given the study’s objective: to assess how cybersecurity controls are implemented, perceived, and enforced across various institutions. The design enables the collection of both quantitative and qualitative data to capture a comprehensive picture of real-world practices without the use of complex mathematical models as it fits to previous studies in the field (Abbinante and Valentini, Omary and Kyaruzi, Mwakalinga and Mushi).

Quantitative data collected through structured questionnaires will be analyzed using simple descriptive statistics such as frequencies, percentages, and cross-tabulations. These will provide insights into trends and patterns in control adoption, staff training, threat awareness, and institutional support across MFS providers and regulators.

Qualitative data from interviews and document reviews will be analyzed thematically to capture deeper insights into enforcement challenges, policy gaps, and organizational experiences. This will enrich the understanding of institutional dynamics and contextual factors influencing cybersecurity effectiveness.

Overall, the descriptive research design allows for a straightforward yet thorough analysis of cybersecurity control implementation in the MFS sector, supporting evidence-based recommendations for policy and institutional improvement.

* 1. **Study Area and Target Population**

The study will be conducted in seven urban centers across Tanzania, selected based on their prominence in mobile financial service activity and diversity of stakeholder presence. These include: Dar es Salaam, Arusha, Mbeya, Zanzibar, Dodoma (Emerging smart city), Mtwara and Singida. These locations offer a representative mix of urban economic hubs, policy centers, and emerging digital markets. The target population includes: Mobile money providers (e.g., Airtel, Vodacom, Mixx by Yass, Halotel), Commercial banks and fintech institutions, Regulatory bodies (e.g., BoT, TCRA, NICTA, FIU, Ministry of ICT), Cybersecurity experts and law enforcement (e.g., FCC, Tanzania Police Force) and end-users of mobile financial services.

* 1. **Theoretical Framework**

The study is grounded in the Technology-Organization-Environment (TOE) framework, which adopts a **descriptive research design** to evaluate the effectiveness of cybersecurity controls in Tanzania's mobile financial services sector. The design provides a holistic view of the technological, organizational, and environmental drivers of cybersecurity control effectiveness. Additionally, Protection Motivation Theory (PMT) is integrated to assess behavioral compliance with security practices among employees and end-users.

* 1. **Data Collection Methods**

|  |  |
| --- | --- |
| **Method** | **Justification** |
| Document review | examining regulatory frameworks, cybersecurity policies, audit reports, and national strategies for understanding environmental and organizational factors. |
| Questionnaires and Surveys | To collect standardized, quantifiable data from IT/security personnel, mobile money providers, bank employees, and regulators for assessing the perceived effectiveness of controls. |
| Interviews | In-depth insights from key informants (cybersecurity officers, regulators) about barriers, effectiveness, and practical experiences, enablling thematic exploration aligned with TOE and PMT. |

The data collection process ensures comprehensive coverage of key research constructs while maintaining methodological rigor. It involves the document review (policies, audits, regulations), questionnaires and surveys (with banks, telecoms, regulators, or consumers), and interviews (key informants such as IT/security officers, policymakers).

* 1. **Sampling Strategy**
* Purposive sampling targets knowledgeable stakeholders (cybersecurity experts at banks, telecoms, regulatory bodies like BoT, TCRA, NICTA, FIU, Ministry of Information and technology, FCC, Tanzania Police Force). Ensures relevance and depth. This will be used to select institutions and individuals with direct cybersecurity responsibility.
* Stratified sampling ensured representation across banks, telecom operators, and urban vs. rural settings by comparing across sectors (banks vs. telecoms) or locations (urban vs. rural). This combined sampling ensures both depth (expert perspectives) and breadth (comparisons across sectors/regions).
  1. **Research Scope**

This study is limited to evaluating cybersecurity control mechanisms within the MFSsector in Tanzania. It focuses on identifying the cybersecurity controls adopted by service providers, evaluating their adequacy and performance, and assessing how these controls align with regulatory expectations and global cybersecurity standards.

The scope encompasses: Mobile service providers (e.g., Airtel, Vodacom, Mixx by Yass), Financial institutions offering MFS (e.g., banks, fintechs), National regulatory and enforcement bodies and Consumer-level engagement on cybersecurity behaviors.

Thematic boundaries include: Technical cybersecurity controls, Organizational cybersecurity governance, Regulatory compliance and enforcement and user perception and behavioral responses to cybersecurity threats

A sample size of at least 150 users and 100 institutional representatives is targeted. The target population includes banks, telecoms, regulators, and consumers of mobile financial service.

* 1. **Data Analysis**

The study employs a mixed-methods data analysis approach, integrating both quantitative and qualitative data to provide a comprehensive understanding of cybersecurity control effectiveness in Tanzania’s mobile financial services (MFS) sector. This approach ensures that numerical trends and stakeholder experiences are analyzed in parallel, offering both breadth and depth to the research findings.

Quantitative data collected through structured questionnaires will be analyzed using Statistical Package for the Social Sciences (SPSS). Descriptive statistics, including frequencies, percentages, means, and cross-tabulations, will be used to identify trends and assess stakeholder perceptions of the adequacy and performance of cybersecurity controls. Likert-scale responses will allow for the quantification of variables aligned with the TOE and PMT frameworks, such as the prevalence of multi-factor authentication, perceived control adequacy, and institutional readiness.

Simultaneously, qualitative data obtained from interviews with key informants (such as ICT officers, regulators, and cybersecurity professionals) and document reviews (including policies, audits, and regulatory reports) will be subjected to thematic analysis using NVivo software. Thematic coding will help identify recurring themes such as implementation challenges, regulatory enforcement gaps, and stakeholder perceptions of control effectiveness. These themes will be aligned with constructs from the TOE, PMT, and RBV frameworks to ensure theoretical coherence.

To ensure robustness and validity, the study will employ triangulation by cross-verifying insights from quantitative and qualitative data sources. For example, if survey data indicate low effectiveness in SIM-swap prevention, and interviewees cite weak identity verification systems as a barrier, these findings will reinforce each other. This triangulated analysis strengthens the reliability of the results and allows for richer interpretation of the cybersecurity landscape in the MFS sector. Overall, the integrated data analysis strategy provides a multidimensional view of cybersecurity practices, performance gaps, and regulatory effectiveness. It supports evidence-based conclusions and actionable recommendations that reflect both measurable outcomes and lived experiences within the mobile financial ecosystem.

* 1. **Research Ethical Considerations, Accuracy, Reliability and Data Validity**

Informed consent will be obtained from all participants, who will participate voluntarily. Confidentiality and anonymity are guaranteed. Ethical clearance will be sought from the appropriate institutional review board before fieldwork. Data will be securely stored and utilized solely for academic purposes. This research ensures ethical compliance by protecting participant confidentiality, obtaining informed consent, and adhering to data protection regulations, including Tanzania’s Cybercrimes Act (2015), by ensuring data reliability through triangulation of sources, conducting validity checks via pre-testing survey instruments, and limiting bias by anonymizing responses and employing diverse data sources.

* 1. **Limitations**

The research may face limitations such as Data access restrictions/ challenges in obtaining sensitive data; limitations related to the reliability of self-reported data, particularly in the case of financial institutions and regulators; potential bias in self-reported data from MFS providers due to security incidents concerns; technological constraints and rapidly evolving cyber threats may affect the research’s findings.

# Research activities, duration, work plan and budget estimate

* 1. **Activities schedule and duration**

This schedule ensures a systematic approach to addressing the research objectives and allows for thorough investigation and analysis of Cybersecurity threats and mitigation measures for mobile financial services in Tanzania. Table 1. 0. below presents a Work Plan chart illustrating the activities.

# References

African Union Cybersecurity Strategy (African Union, 2020).

Bank of Tanzania. (2023). Report on emerging threats in digital financial services.

Bank of Tanzania (BoT) Cybersecurity Guidelines (2022).

Barney’s (1991) Resource-Based View (RBV) of Competitive Advantage.

Cybercrimes Act. (2015). The Cybercrimes Act, Tanzania. Government of Tanzania.

Cohen and Felson (1979) Routine Activity Theory (RAT).

European Union Agency for Cybersecurity (ENISA). (2022). Annual cybersecurity report. ENISA.

EADB. (2022). Cybersecurity framework for financial inclusion in East Africa. EADB.

EACO. (2021). Regional cybersecurity strategies and best practices. EACO.

GSMA. (2021). State of mobile financial services fraud in Sub-Saharan Africa. GSMA.

GSMA. (2022). Evaluation of MFS cybersecurity measures in emerging markets. GSMA.

Institutional Theory (Scott, 1995).

INTERPOL. (2020). African cyber threat assessment report. INTERPOL.

Kenya’s Central Bank (CBK, 2021) cybersecurity guidelines for mobile payment service providers.

Klapper, L., Ansar, S., Hess, J., and Singer, D. (2022). Mobile money and digital financial inclusion.

Malabo Convention (African Union, 2014).

McKinsey and Company. (2022). Public-private partnerships (PPPs) in cybersecurity within Africa.

Mwakalinga, A., and Mushi, M. (2020). Cybersecurity threats and mitigation strategies in mobile money transactions in Tanzania. Tanzania Journal of ICT.

Omary, S., and Kyaruzi, M. (2022). Evaluating the implementation of Tanzania’s national cybersecurity policy in the financial sector. University of Dar es Salaam Press.

Permanent Secretary, President’s Office, Public Service Management and Good Governance. (2022). Government cybersecurity strategy 2022–2027. Government of Tanzania.

SADC (2020). SADC Mobile money guidelines. SADC Secretariat.

Tanzania Cybersecurity Centre (TCC). (2022). Annual cybersecurity risk report.

TCRA. (2022). Annual cybersecurity incidents report in Tanzania.

Verizon. (2023). Data breach investigations report. Verizon.

**Appendix**

**Table 1.0. Research activities plan**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **MONTHS** | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Literature Review |  |  |  |  |  |  |  |  |  |  |  |  |
| Data Collection |  |  |  |  |  |  |  |  |  |  |  |  |
| Data Cleaning/Analysis |  |  |  |  |  |  |  |  |  |  |  |  |
| Report Writing |  |  |  |  |  |  |  |  |  |  |  |  |
| Buffer/Revision |  |  |  |  |  |  |  |  |  |  |  |  |
| Final Edits/Proofing |  |  |  |  |  |  |  |  |  |  |  |  |
| Submission Prep |  |  |  |  |  |  |  |  |  |  |  |  |
| Final Submission |  |  |  |  |  |  |  |  |  |  |  |  |

* 1. **Research Budget Proposal**

|  |  |
| --- | --- |
| **Activity** | **Cost (TZS)** |
| Literature review | 2,000,000.00 |
| Data collection | 8,500,000 |
| Field transport | 3,000,000 |
| Data Analysis & Report Writing | 3,000,000 |
|  |
|  |
| Draft report writing |  |  |
| Perdiem researchers | 3,500,000 |  |
| **Cost** | **20,000,000.00** |  |

**Annex I: RESEARCH QUESTIONNAIRES**

Dear Respondent, we, Eng. Bernard Kambanga, Eng. Dr. Romwald Lihakanga (PhD) and Emmanuel Kajange, conducting research titled “Assessment of Cybersecurity Controls in Mobile Financial Services (MFS) in Tanzania “we kindly request you to complete this questionnaire with appropriate answers and the information provided will be kept confidential and will be used only for academic purposes. We would be thankful if you will help me get appropriate answers in this questionnaire. We expect your kind support in this aspect.

**A. Questionnaire (Quantitative)**

**Instrument Type**: Closed-ended questions (mostly Likert-scale from 1–5; 1 = Strongly Disagree, 5 = Strongly Agree or Binary Yes/No)

**Section A: Background Information (Demographics and organizational profile)**

1. What type of organization do you represent? (Bank, Telecom, Fintech, Regulator, Other - specify)
2. What is your role in the organization? (ICT Officer, Compliance Officer, Executive, etc.)
3. How many years has your organization been operating in the MFS sector?
4. What is the approximate size of your customer base for mobile financial services?
5. Has your organization experienced any cyber-related incident in the past 12 months? (Yes/No)

**Section B: Identification of Controls (TOE – Technology Context)**

1. Our organization has implemented multi-factor authentication (MFA) for MFS users.
2. End-to-end encryption is enforced across all MFS communication channels.
3. Our MFS systems undergo regular penetration testing and security audits.
4. We have deployed real-time transaction monitoring systems to detect suspicious activities.
5. Security patches and software updates are applied timely to MFS platforms.

**Section C: Adequacy Assessment (TOE + PMT)**

1. The cybersecurity controls implemented are sufficient to prevent most common cyber threats.
2. Our cybersecurity infrastructure aligns well with international standards (e.g., ISO 27001, PCI DSS).
3. Budget allocation for cybersecurity in MFS is adequate and consistent.
4. The current legal/regulatory environment adequately supports cybersecurity in the MFS sector.
5. Staff are regularly trained and updated on cybersecurity policies and practices.

**Section D: Performance Indicators (TOE + PMT: Response Efficacy, Self-Efficacy)**

1. Our current cybersecurity measures are effective in reducing fraud and unauthorized access.
2. There has been a measurable reduction in security incidents over the past year.
3. Our team is confident in their ability to detect and respond to cybersecurity threats.
4. We regularly monitor and evaluate the performance of our security controls.
5. Management provides timely support and resources for cybersecurity incidents.

**Section E: Behavioral Factors and Motivation (PMT)**

1. I believe cybersecurity threats to mobile financial services are serious and increasing.
2. I feel personally responsible for ensuring cybersecurity in my organization.
3. The consequences of a cybersecurity breach are well understood in our organization.
4. I am motivated to follow security policies even when not being monitored.
5. Organizational culture encourages proactive behavior toward cybersecurity.

**B. Interview Guide (Qualitative)**

**Instrument Type**: Open-ended, exploratory questions

**1. Strategic Choices in Control Selection**

1. What factors guide your organization’s selection of cybersecurity controls for mobile financial services?
2. Can you describe how technological trends or limitations have influenced your control decisions?
3. How do you assess the risks that guide which cybersecurity controls to prioritize?
4. To what extent do financial, organizational, or human resource constraints affect your choices?
5. What role do customer trust and usability concerns play in implementing specific security measures?

**2. Regulatory Compliance Challenges**

1. How does your organization ensure compliance with national cybersecurity regulations in the MFS sector?
2. What challenges do you face in interpreting or implementing regulatory requirements?
3. Are there any specific policies or legal gaps that hinder your cybersecurity efforts?
4. How responsive are regulators to the evolving nature of cybersecurity threats in the mobile finance space?
5. What recommendations would you make to improve regulatory frameworks for better cybersecurity outcomes?

**C: Checklist Questionnaire for Regulatory and Government Stakeholders**

This checklist is designed to gather concise responses from key regulatory and government institutions involved in overseeing cybersecurity in Tanzania’s Mobile Financial Services (MFS) sector, including BoT, TCRA, the Ministry of Information and Technology, and FCC. Each item should be addressed briefly (2–3 sentences), drawing on institutional experience and frameworks. The responses will support analysis of policy enforcement, coordination, institutional capacity, monitoring practices, and strategic readiness within the sector.

#### **A. Policy and Legal Framework**

1. Does your institution have a comprehensive cybersecurity regulatory framework in place for mobile financial services?
2. Are there clearly defined mechanisms for enforcing penalties in cases of cybersecurity non-compliance in the MFS sector?
3. How often are cybersecurity-related laws and regulations updated to reflect emerging digital threats?
4. To what extent are national cybersecurity regulations aligned with international standards (e.g., ISO 27001, GDPR, PCI-DSS)?
5. How does your institution communicate cybersecurity obligations to regulated MFS providers?

#### **B. Institutional Coordination and Stakeholder Engagement**

1. Is there a formal inter-agency coordination mechanism in place to manage cybersecurity in the MFS ecosystem?
2. How regularly does your institution collaborate or meet with other stakeholders (e.g., BoT, TCRA, MITI, FCC) to address cybersecurity issues?
3. In what ways does your institution collaborate with MFS providers to support cybersecurity practices?
4. Does Tanzania have a centralized body or taskforce responsible for national MFS cybersecurity coordination?
5. Are there standardized procedures across institutions for reporting and responding to cybersecurity incidents?

#### **C. Capacity and Resources**

1. Does your institution have dedicated unit or personnel responsible for cybersecurity oversight and coordination?
2. How frequently are cybersecurity staff trained or upskilled on emerging technologies and threat landscapes?
3. What tools or systems does your institution use to conduct audits, vulnerability assessments, or compliance checks?
4. Is there a designated budget line within your institution specifically allocated for cybersecurity regulatory activities?
5. Has your institution participated in national or regional cybersecurity drills, simulations, or joint exercises?

#### **D. Monitoring and Evaluation of Cybersecurity Controls**

1. Does your institution receive periodic cybersecurity compliance reports from MFS providers?
2. How frequently does your institution conduct on-site inspections or assessments of MFS cybersecurity controls?
3. Are there performance indicators in place to evaluate the effectiveness of your institution’s regulatory enforcement?
4. How is trend data on incidents such as phishing, SIM-swap fraud, or mobile money fraud analyzed and acted upon?
5. Are post-incident reviews and policy updates conducted after major cybersecurity breaches?

#### **E. Strategic and Future Readiness**

1. Does your institution have a medium- or long-term cybersecurity strategy or roadmap guiding future interventions?
2. To what extent do current regulatory models accommodate future innovations (e.g., digital IDs, blockchain, AI-driven financial services)?
3. Has your institution been involved in public cybersecurity awareness or consumer protection campaigns?
4. Are there any active partnerships between your institution and academic/research organizations focused on cybersecurity policy or implementation?
5. How is cybersecurity integrated into Tanzania’s broader digital transformation and ICT development strategies?

**Annex II: CURRICULUMS VITAE**

* 1. **Eng. Bernard Makungu Kambanga**

Principal Electrical Engineer Bank of Tanzania Mwanza Branch, Email: [bmkambanga@bot.go.tz](mailto:bmkambanga@bot.go.tz)**.**

**Education:** Master’s in Business Administration –Corporate Management is (MBA-CM) (2009-2011) Mzumbe University; Bachelor of Engineering (BEng.) in Electronics and Telecoms (2005-2008) Dar es Salaam Institute of Technology (DIT); Full technician certificate (FTC) in Electronics and Telecoms (1998-2001)- Dar es Salaam Institute of Technology (DIT); CSE 1994-1997-Iyunga Technical Secondary, Mbeya.

**Skills:** Diverse Electronics and Telecommunication registered professional Engineer (**Registered ERB Tanzania-2014**).

**Work Experience at Bank of Tanzania:** July 2024 –To date Principal Engineer; June 2019-June 2024 Senior Engineer/ supervisor - Facilities and Estate Division Mwanza Branch.

**Certifications:** Nice Systems (CCTV) technical course, Eckoshield hfc227ea/ Inergen product, Open Transport Network (OTN) course, Training in Security Systems by M/S Itakane Johannesburg South Africa, Dintek Certified Installer Training.

**Professional Bodies:** Engineers Registration Body (ERB-Tanzania reg# 3891-Professional Engineer); Institution of Engineers Tanzania (MIET).

**References: on request**

* 1. **Dr. Romwald Lihakanga**

Electronics and Telecommunication Department, Dar es salaam Institute of Technology.

Email: romwald.lihakangaa@dit.ac.tz

**EDUCATION**: 2018 – 2022 Heriot Watt University (Edinburgh, United Kingdom)-PhD. In Sensors and Systems; 2011 – 2012: University of Glamorgan (Wales, United Kingdom)- Masters of Science in Electronic Product Design (Graduated with Distinction); 2005 – 2009: DIT -BEng. in Electronics and Telecommunication Engineering -Upper Second Class; 2000 – 2003: DIT – FTC in Electronics and Telecommunication Engineering

**RESEARCH EXPERIENCE:** 2018 – Present: Heriot Watt University (Edinburgh, United Kingdom), PhD. Dissertation Research - Thesis Advisers: Professor Gabriela Medero, Dr. Yuan Ding a Generic Wireless Sensor Network for Dynamic Variation of Building Material.

**PROFESSIONAL BODIES:** Registered by Engineers Registration Body (ERB-Tanzania reg# 3727) as Graduate Engineer; Registered by Institute of Engineers Tanzania (IET-Tanzania reg # ST/1267/2008) as a student; Registered by Institute of Electrical and Electronics Engineers (IEEE-reg# 97010060) as a student member.

**OTHER JOB EXPERIENCE:** 2008 –2009 System Engineer/Site Engineer/Project Manager - Hexatech Company Tanzania Limited (Dar es salaam, Tanzania). 2003-2008 Signals, Electronics and Telecommunication Engineer /Military Officer/ Correctional Officer - Tanzania Prisons Service (Dar es salaam, Tanzania).

**LIST OF REFERENCES:** Available on Request

* 1. **Emmanuel Sefania Kajange**

[emmanuel.kajange@dit.ac.tz](mailto:emmanuel.kajange@dit.ac.tz)

**EDUCATION BACKGROUND:** Sept 2020 – Dec 2021 (University of Birmingham)- Master of Science in Cyber security; Oct, 2010-Jan, 2015 DIT -BEng.in Electronics and Telecommunication engineering; 2008-2010 Moshi technical Secondary School- ACSEE, 2004-2007 Pamba Secondary School) - CSEE.

**WORK EXPERIENCE: 2022 – Present** Company: Dar es Salaam Institute of Technology (DIT); Position: Assistant Lecturer, Telecommunication

**PAST EXPERIENCE:** Project member (2023 - present), Security management assessment at Dar es Salaam Institute of Technology; Project (2022), Security analysis of the LoRAWAN protocol; Conduct Cyber security professional training; Research fellow, Design a Low Power Wide Area Network (LPWAN) adaptive network

**PERSONAL SKILLS:** Cyber security: security assessment, malware analysis, reverse engineering, software security analysis and security management; Electronics systems design and fabrication

**REFEREES**: available on request