EVALUATING THE IMPLEMENTATION OF CBK CYBERSECURITY GUIDELINES AND THEIR EFFECT ON ONLINE BANKING SECURITY: INSTITUTIONAL RESOURCES AS A MEDIATING FACTOR

LOICE WACHUKA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF COMMERCE OF STRATHMORE UNIVERSITY, NAIROBI, KENYA

MAY, 2025

DECLARATION

Student's Declaration

This Thesis is my original work and has not been submitted for academic recognition or presented in any other university for any academic award.

Signature  Date 20 May 2025

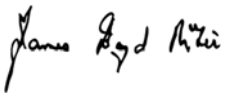
Loice Wachuka

114441

Supervisor's Declaration

This thesis has been submitted for examination with my approval as the University supervisor.

Signature



Date 20 May 2025

Dr. James McFie

Strathmore University

DEDICATION

I dedicate this study to my family. You have been a consistent source of love, encouragement and unwavering support throughout this quest and beyond. I am and will be eternally thankful for the unwavering encouragement to pursue my aspirations.

ACKNOWLEDGEMENT

First and foremost, I am thankful to my supervisor for his unwavering support during the drafting of my thesis. He provided me the information and abilities that were needed to completing my thesis successfully. I would want to recognize and thank everyone who motivated me and who guaranteed that I accomplished this research thesis effectively. The instructors at Strathmore University must be recognized for their efforts. They have devoted their time and energy to ensuring that I comprehend the course. My gratitude also goes to my family more so, my children for their never-ending inspiration, unshakable support and unrelenting encouragement during the process of penning my thesis. Thank you, and may God bless every one of you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This study investigates the effectiveness and extent of implementation of the Central Bank of Kenya's Guideline on Cybersecurity for Payment Service Providers (GCPSP), issued in July 2019, with a specific focus on its role in enhancing the security of online banking transactions in Kenya. The purpose of the study is to assess how well these guidelines have been implemented by commercial banks, evaluate their impact on cybersecurity outcomes, and examine the mediating role of institutional resources in influencing their effectiveness. The research was guided by five key objectives: to determine the extent of access control measures implementation; to establish the degree to which incident response mechanisms have been put in place; to examine the integration of data protection protocols; to assess the application of network security standards; and to investigate the moderating effect of institutional resources on the relationship between GCPSP implementation and the security of online banking in commercial banks. The study focused on 38 commercial banks and 1 mortgage finance company, which has transitioned from being a mortgage financier to a provider of integrated financial solutions with interests in Personal Banking, SME and Commercial Banking (HF Group Overview, 2025). The headquarters of all these financial institutions are situated within the Nairobi metropolitan area. The study was anchored in Diffusion of Innovation Theory and Agency Theory. A descriptive survey design was employed, targeting 429 individuals involved in online transaction monitoring, with a final sample of 220 respondents. Data was collected using structured questionnaires and analyzed using SPSS. The findings revealed that access controls, incident response mechanisms, data protection protocols and network security standards significantly contribute to secure online banking. Additionally, institutional resources (financial, technological, and human) were found to moderate the effectiveness of GCPSP implementation. The study was constrained by strict timelines, which limited respondent engagement and required a streamlined data collection process within the academic schedule. The research offers actionable insights for policymakers and financial institutions seeking to strengthen cybersecurity compliance and resilience in Kenya's digital banking sector.

CHAPTER ONE
INTRODUCTION

1.1 Background to the Study

Online banking has revolutionized financial services globally by providing customers with convenient, secure and seamless access to banking operations through digital platforms (Khan, 2021). This innovation has significantly improved access to financial services, increased transactional efficiency and redefined how banks interact with their customers (Okifo, 2021). However, despite these advantages, online banking comes with inherent risks, particularly related to cyber security. Cyber threats such as phishing, distributed denial-of-service (DDoS) attacks, identity theft and financial fraud have become increasingly prevalent, eroding public trust in digital banking systems (Brar, 2022). The rapid advancement of technology has not only amplified these risks but also highlighted vulnerabilities in existing systems (Kaur, 2020). These challenges emphasize the critical need for robust regulatory frameworks to ensure secure online transactions, thereby sustaining confidence in the financial sector (Khan, 2021). Consequently, global financial regulators are prioritizing cyber security to protect customers and ensure the stability of financial institutions (Ntim, 2021).

Globally, countries have implemented regulatory frameworks to secure online banking systems and mitigate cyber security threats. For instance, the European Union introduced the General Data Protection Regulation to ensure the protection of customer data, while the Payment Service Directive 2 mandates strong customer authentication across digital platforms (Huth, 2020). In the US, the Federal Financial Institution Examination Council has provided guidelines on risk management, incident response and secure system configurations (Jones, 2023). These measures have successfully minimized fraud, protected consumer data and reinforced public trust in the digital banking systems (Bansal, 2022). However, high implementation costs, rapid technological changes and complex cyber threats remain persistent challenges for regulatory bodies and financial institutions worldwide (Okonkwo, 2019). A notable example is the 2020 cyberattack involving North Korean hackers who launched a malware attack named ATMD Track targeting Indian ATMs and banking institutions, intending to steal payment information (Singh & Kumar, 2020). These obstacles highlight the need for continuous improvement in global cybersecurity standards to address emerging risks effectively (Bansal, 2022).

In Africa, several countries have adopted international cybersecurity standards to protect their financial systems from digital vulnerabilities. For example, South Africa and Nigeria have implemented frameworks like ISO 27001 to strengthen online banking systems and address cyber threats (Adeyemi, 2021). These initiatives have proven effective in reducing fraud, enhancing customer data protection and improving the overall reliability of banking services (Okonkwo, 2019). However, the adoption of these measures has not been without challenges. Limited resources, infrastructure gaps and regulatory inconsistencies have hindered the full realization of these frameworks in many African nations (Amankwah-Amoah, 2020). There is a growing need for regional collaboration and capacity-building initiatives that enhance cybersecurity across the continent (Dlamini, 2023). Institutional resources, including financial investment, advanced technological infrastructure and skilled human capital, play an essential part in supporting the effective application of these cybersecurity frameworks (Osaji,2021). Without sufficient institutional backing, the effectiveness of cybersecurity initiatives can be significantly compromised.

In Kenya, significant strides have been made to improve the security of online banking through the CBK's implementation of the Guideline on Cybersecurity for Payment Service Providers (GCPSP) (Njogu, 2023). This guideline mandates financial institutions to adopt multi-factor authentication, conduct regular risk assessments and ensure encryption of customer data to mitigate cyber security threats (CBK, 2019). Its implementation has involved mandatory staff training programs to enhance awareness of cyber risks, establishment of dedicated cyber security teams and investments in advanced technological systems like intrusion detection and prevention mechanisms (Mukami, 2021). Banks are also required to submit regular compliance reports to the CBK and undergo routine audits to ensure adherence (Wairimu, 2022). However, challenges persist, including uneven adherence to regulations, inadequate enforcement capacity and the rapid evolution of cyber threats (Wamuyu, 2020). Smaller banks often struggle to meet these requirements due to limited financial and technical resources, creating disparities in implementation (Muthoni, 2021). Additionally, the fast-paced development of cyber threats necessitates constant updates to the guidelines and swift responses, which can strain institutional resources (Gichuki, 2022). One glaring example of these vulnerabilities was the $2.1 million debit

card fraud at Equity Bank in 2024, where hackers exploited weaknesses in the bank's security systems, highlighting the ongoing risks and gaps in the protection of online banking transactions.

Between July and September 2024, the National KE-CIRT/CC reported a surge in several categories of cyber threats targeting Kenya's critical information infrastructure. Malware threat attempts rose to 33.9 million, a 6.13% increase from the previous quarter, primarily affecting the ICT sector and cloud service providers. Web application attacks increased by 18.62% to 174,251 attempts, targeting government systems and exploiting SSL/TLS misconfigurations. Brute force attacks saw a significant rise of 42.01%, with over 38 million attempts focused on compromising login credentials and database servers, particularly in government and cloud-based systems. Mobile application attacks also grew by 18.5%, largely targeting Android devices through malware. In contrast, Distributed Denial-of-Service (DDoS) attacks sharply declined by 75.10% to 1.83 million incidents, although they still posed a risk to government and health sector infrastructure through protocol exploitation and service disruption attempts.

To address these challenges and further strengthen online banking security, Kenya's financial sector must invest in modern technologies, enhance personnel training and establish more robust monitoring and evaluation frameworks (Omondi, 2023). This study attempted to evaluate the effectiveness of the regulating body framework and to establish to what extent the GCPSP have been implemented providing actionable insights to enhance cyber security in Kenya's commercial banks.

1.1.1 The CBK Guidelines

The Central Bank of Kenya (CBK) introduced the Management Guidelines in 2019 to address growing concerns about cyber security within the financial sector (Nyambura, 2020). The primary aim of these guidelines was to enhance the security of online banking transactions by establishing clear directives that financial institutions must follow to mitigate emerging cyber threats and safeguard customer data within digital banking systems (Kamau, 2020). The guidelines were designed to ensure that banks were not only equipped to handle the risks associated with cyber security, but also had the necessary technological and operational measures in place to protect their systems and customers (Wanjiru, 2020). The CBK's regulatory response was rooted in the recognition of the increasing sophistication of cyber threats, which were undermining trust in

digital banking (Njoroge, 2020). Over time, these guidelines have been updated, with the most recent revision taking place in 2019 to address new and evolving challenges in the cyber security landscape (Ngugi, 2020). CBK continues to emphasize the importance of maintaining a proactive approach to managing these risks, which are seen as critical for the ongoing stability of the financial sector (Mutua, 2020). This continuous refinement of the guidelines reflects the changing nature of cyber threats and the need for financial institutions to stay ahead of technological advancements to ensure secure online banking (Mwangi, 2020).

The CBK is responsible for conducting regular audits and reviews to assess whether banks have fully implemented the required cyber security measures (Mwangi, 2020). This oversight role is vital to ensuring that all financial institutions adhere to the guidelines and meet the necessary security standards (Okoth, 2020). However, while the CBK has made considerable progress in monitoring compliance, several challenges remain (Ochieng, 2020). One of the most significant obstacles is the inconsistency in enforcement, particularly among smaller financial institutions that face resource constraints (Njeru, 2020). These tier three banks often struggle to meet the standards set by the CBK due to limited financial and technical resources, which creates disparities in the implementation of the guidelines (Omondi, 2020). First tier banks, on the other hand, are better equipped to implement the necessary cybersecurity measures, which has led to a situation where not all financial institutions are equally protected against cyber threats (Nyambura, 2020). Moreover, the rapid evolution of cyber threats presents an ongoing challenge for CBK in terms of updating the guidelines and responding swiftly to emerging risks (Kamau, 2020). While the CBK's efforts are commendable, the persistence of challenges in enforcement and continuous emergence of new cyber threats highlight the need for further investment in resources and capacity-building initiatives (Wanjiru, 2020). Ensuring uniform compliance across all financial institutions is essential for enhancing the overall security of online banking transactions in Kenya and fostering customer confidence in the financial sector (Njoroge, 2020).

1.1.2 Security of Online Banking Transactions in Kenya

The security of online banking transactions in Kenya has become a priority for both financial institutions and regulatory bodies as the country increasingly adopts digital banking systems (Gikandi & Bloor, 2020). With the rise in digital financial services, ensuring confidentiality,

integrity and availability of online banking data has become essential for maintaining customer trust (Mutuku, 2020). In response to the growing demand for secure online transactions, various measures have been implemented by Kenyan banks to address cyber threats and safeguard financial transactions (Muriuki, 2020). The Central Bank of Kenya (CBK) has taken the lead in ensuring the security of digital banking by issuing compliance Management Guidelines, which require financial institutions to adopt a set of security measures designed to protect customers from fraud and cybercrime (Makau & Wambua, 2020).

The banking sector in Kenya is confronted with several cybersecurity threats that compromise the security of online banking transactions (Lwamba, 2020). Phishing attacks have become widespread, where fraudsters impersonate bank personnel to trick customers into divulging sensitive financial information such as account numbers and passwords (Kariuki, 2020). Additionally, the country has witnessed a surge in identity theft cases, where cybercriminals steal personal information to carry out fraudulent transactions or open fake accounts (Njoroge & Mwangi, 2020). Malware attacks are also common, with malicious software being used to infiltrate banking systems, thereby allowing unauthorized access to sensitive financial data (Omondi, 2020). DDoS (Distributed Denial of Service) attacks are another major concern, where cyber attackers flood the banks' websites with excessive traffic, rendering them inaccessible to legitimate customers (Karanja, 2021). These threats highlight the vulnerability of online banking systems in Kenya, necessitating constant vigilance and improvement of security measures to prevent cybercrime (Muriuki & Wambua, 2020). Cyber risks have increased due to the digitisation of making payments and transfer of money from person to person. The cyber threats were high in 2022/23 and increased in between June 2023 and March 2024 than the threats reported in 2021/2022. System misconfiguration had the highest increase in 2022/23 and 2023/ 202424 (March) while DDOS threats were the lowest. Kenya Financial Stability Report (2024).

In response to these emerging threats, Kenyan financial institutions have taken proactive steps to mitigate cyber risks (Gikandi & Bloor, 2020). The adoption of multi-factor authentication (MFA) has been one of the most widely implemented strategies, requiring users to authenticate their identity using multiple methods such as PINs, one-time passwords (OTPs) and biometric features (Makau, 2020). Additionally, banks have invested in encryption technologies to ensure protection of sensitive data during transactions, making it unreadable to unauthorized parties (Ochieng &

Karanja, 2020). Financial institutions have also adopted advanced intrusion detection and prevention systems (IDPS), which monitor their networks for suspicious activities and block potential threats in real-time (Njoroge & Mwangi, 2020). Despite these efforts, the ongoing evolution of cyber threats poses challenges to maintaining a secure online banking environment (Kariuki, 2020). To strengthen cybersecurity in Kenya's banking sector, continuous monitoring, regular system audits and customer education on secure online practices are necessary (Lwamba, 2020).

1.1.3 Commercial Banks in Kenya

Commercial banks in Kenya play a pivotal role in the country's financial ecosystem by offering a wide range of services, including savings and current accounts, loans, mortgages and facilitating payment systems (Odhiambo, 2021). The Central Bank of Kenya (CBK) regulates these institutions and aims to ensure financial stability while protecting customer interests (Central Bank of Kenya [CBK], 2020). The banking sector has experienced significant growth over the years, with both local and international banks operating in the country (Wakoli, 2024). As of 2020, there are 38 commercial banks and 1 mortgage finance company in Kenya, contributing to financial inclusion by providing services to both urban and rural populations (Kenya Bankers Association [KBA], 2020). Kenya's banking sector is categorized into small (Tier III), medium (Tier II) and large (Tier I) peer groups in terms of their market share. Kenya Financial Stability Report (2023).First tier banks such as Kenya Commercial Bank (KCB), Equity Bank and Cooperative Bank dominate the sector, offering a variety of financial products (Wakoli, 2024).

1.2 Statement of the Problem

The issuance of the Central Bank of Kenya (CBK) Guideline on Cybersecurity for Payment Service Providers (GCPSP) in July 2019 was a significant step towards strengthening the security of online banking transactions. However, this guideline has not been fully implemented across the banking sector, particularly among 2nd and 3rd tier banks. Cyber threats continue to rise, with 1.1 billion threat events detected in Kenya between April and June 2024 - a 16.5% increase from the previous period as per the CAK (2024). This increase reflects the growing risks faced by financial institutions in the country, highlighting the urgent need for more robust security measures, yet many banks still fall short in fully adopting the necessary practices.

The implementation of security guidelines, such as the General Compliance & Security Protection Standards (GCPSP), is significantly impacted by various factors, particularly in the banking sector (Central Bank of Kenya; Bank Supervision Dept, 2023). While tier 1 banks have the resources to integrate advanced security measures like multi-factor authentication (MFA), encryption, and regular risk assessments, smaller 2nd and 3rd tier banks face challenges in these areas. Limited financial resources hinder their ability to invest in the necessary cybersecurity infrastructure, leaving them vulnerable to threats such as phishing attacks and unauthorized access. Additionally, smaller banks often struggle with outdated legacy systems that cannot support modern security protocols, further complicating compliance efforts (Kariuki, 2015). These institutions may lack the skilled personnel needed to implement and maintain robust security measures. Tier 1 banks, on the other hand, benefit from a well-established compliance culture, dedicated teams, and access to advanced tools that ensure comprehensive risk mitigation (Central Bank of Kenya. Bank Supervision Dept, 2023). In contrast, 2nd and 3rd tier banks may not have the capacity for frequent risk assessments, incident response plans, or the ongoing training required to safeguard against cyber threats. While larger banks are better positioned to meet regulatory standards and protect sensitive data, smaller institutions are at a greater risk of falling behind in their cybersecurity practices, leaving them vulnerable to persistent online banking risks.

The GCPSP requires multi-factor authentication, encryption and regular risk assessments, which are essential for mitigating online banking risks. While 1st tier banks have made progress in implementing these measures, the majority of 2nd and 3rd tier banks struggle with access control mechanisms, data protection protocols, incidence response, network security standards and institutional resource capability. This leaves them vulnerable to persistent threats like phishing scams and unauthorized access to customer accounts (Velasco, 2024).

In addition, 75% of vulnerabilities in the sector are linked to unpatched systems and outdated software (Cybersecurity in Financial Sector Development Report, 2020). These ongoing weaknesses indicate that the GCPSP is not being consistently applied across all banking tiers, leaving online banking transactions exposed to cyber threats which may result in financial loss in case of attack. While the statements above point to the status of cyber security implementation in the banks in Kenya, this research seeks to establish the exact position of GCPSP implementation

in the country and to determine whether the GCPSP has truly enhanced the security of online banking transactions in Kenyan commercial banks.

1.3 Objectives of the Study

1.3.1 General Objective

The general objective of this research was to evaluate the extent of implementation of the Central Bank of Kenya (CBK) Guideline on Cybersecurity for Payment Service Providers July 2019 (GCPSP) and assess its impact on the security of online banking transactions in Kenya.

1.3.2 The Specific Objectives include the following:

The specific objectives of this research included:

i. To determine the extent to which access control measures have been implemented to enhance the security of online banking transactions in Kenya.
ii. To establish the degree to which incident response mechanisms have been put in place to improve the security of online banking transactions in Kenya.
iii. To examine the extent to which data protection protocols have been integrated into commercial banks to ensure the security of online banking transactions in Kenya.
iv. To find out the degree to which network security standards been established and applied to secure online banking transactions in Kenya.
v. To investigate the moderating effect of institutional resources on the relationship between CBK guidelines implementation and secure online banking transactions in commercial banks in Kenya.

1.4 Research Questions

The research questions of this study included:

i. To what extent have access control measures been implemented to enhance the security of online banking transactions in commercial banks in Kenya?
ii. How effective are the incident response mechanisms in mitigating risks to the security of online banking transactions in Kenyan commercial banks?
iii. How well are data protection protocols operating in commercial banks in Kenya to safeguard online banking transactions?

iv. To what degree have network security standards been established and applied to secure online banking transactions in commercial banks in Kenya?

v. What is the moderating effect of institutional resources on the relationship between CBK guidelines implementation and secure online banking transactions in commercial banks in Kenya?

1.5 Scope of the study

This study examined the effectiveness of the GCPSP and the degree of its implementation on online banking transactions in Kenya. The study cuts across the Kenya's 38 licensed commercial banks and 1 mortgage finance company. It examined the level of compliance with GCPSP, its effectiveness in mitigating cyber security risks such as fraud and data breaches and the influence towards online banking transaction. The target population included include ICT and compliance personnel within commercial banks and key informants such as CBK officials. The investigation was carried out for a period of two months, February to April 2025.

1.6 Significance of the study

First**,** the research provides insights into how well Payment Service Providers are adhering to the Central Bank of Kenya's Guideline established in July 2019 on Cybersecurity (GCPSP) among commercial banks in Kenya. It highlights potential gaps in its implementation, enabling the Central Bank of Kenya to refine its GCPSP and ensure revisions are practical, comprehensive and effective in addressing emerging cyber security challenges.

In addition, by evaluating the impact of the GCPSP on secure online banking transactions, the study assisted commercial banks in understanding the efficacy of their current compliance measures. The findings guide financial institutions in improving their security protocols, thereby minimizing risks associated with cyber threats, fraud and data breaches.

Further, policymakers and advocacy groups in Kenya benefit from the study’s findings by gaining a clearer understanding of the effectiveness of existing regulations. Having a clearer understanding can help shape robust policies and programs aimed at fostering a more secure as well as resilient financial system. The findings of this study not only be relevant to Kenya but also to other developing countries facing similar challenges in regulating online banking security

1.7 Chapter Summary

The opening chapter provides an overview of the study by outlining the background, problem statement, objectives, research questions, significance and scope. The study focuses on an assessment of the implementation and effectiveness of CBK Cybersecurity guidelines for commercial banks, the mediating role of institutional resources. It highlights the challenges faced by the banks, CBK implementation framework, compromised network security and substantial financial loss in instances of hacking. The chapter highlights the study's importance for policy makers, practitioners and academics by providing actionable insight, policy recommendations and contributions to CBK guidelines.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents the theoretical framework, empirical literature review, conceptual framework, study hypotheses, research gap and summary of literature.

2.2 Theoretical Foundation

The study was anchored on two theories: Technology Acceptance theory, Diffusion of Innovation Theory and Agency Theory.

2.2.1 Technology Acceptance Model (TAM)

TAM was created by Davis (1989) as an expansion of the Theory of Reasoned Action with the purpose to explain and forecast the acceptance and use of technology. TAM assumes that two principal factors, perceived usefulness and perceived ease of use, determine a person's intention to adopt a certain technology. Perceived usefulness refers to the extent of the belief by a person in the helpfulness of using the technology in performing his or her job better. Perceived ease of use, on the other hand, refers to how much a person thinks utilizing the technology will be effortless. According to Davis, Bagozzi, and Warshaw (1989), an individual's attitudes about technology are influenced by these beliefs, and these attitudes in turn impact their behavioral intention and actual use of technology. The model has been widely recognized for its simplicity and applicability in studying technology adoption across diverse settings. Recent studies have extensively applied TAM in various domains. Owusu and Boh (2021) used TAM to investigate elements impacting sub-Saharan Africa's adoption of mobile banking, finding that perceived usefulness significantly impacts user adoption rates. Similarly, Charness and Boot (2020) applied TAM to examine how well e-learning systems are embraced during the COVID-19 epidemic, highlighting the role of perceived ease of use in user engagement. Despite its popularity, TAM has faced criticisms for its limitations. Bagozzi (2007) argued that the model oversimplifies the complexity of technology adoption by focusing narrowly on PU and PEOU, neglecting external factors such as cultural, social, and organizational influences. Furthermore, critics contend that TAM assumes a linear progression from intention to usage, which may not account for real-world inconsistencies in technology adoption.

In this study, TAM is highly important because it provides a theoretical framework for examining how stakeholders in Kenyan commercial banks perceive the CBK's guidelines. The model can help analyze how the perceived efficacy and ease of implementation of these guidelines influence their adoption and compliance by financial institutions. Moreover, TAM offers insights into addressing challenges in securing online banking transactions, as understanding stakeholders' attitudes toward the guidelines can inform targeted interventions to enhance adherence and effectiveness. Through leveraging TAM, this study aims to evaluate the broader factors driving or hindering the successful application of CBK guidelines in the banking sector.

2.2.2 Diffusion of Innovation Theory

The Diffusion of Innovations (DOI) Theory was developed by Everett Rogers in 1962 and has been widely used to explain how innovations are adopted and spread within social systems (Rogers, 2003). The theory postulates that innovation diffusion occurs through a process involving five stages: knowledge, persuasion, decision, implementation, and confirmation. Rogers (2003) identifies five key attributes of innovations that influence adoption rates: relative advantage, compatibility, complexity, trialability, and observability. Additionally, the theory classifies adopters into five categories: innovators, early adopters, early majority, late majority, and laggards. This classification highlights how social networks and communication channels influence the adoption of new technologies, policies, or practices.

Recent studies have applied DOI Theory to various domains, showcasing its adaptability AL-Emran et al. (2020) utilized the theory to explore the adoption of e-learning technologies in higher education institutions, finding that compatibility and relative advantage significantly influence adoption rates. Similarly, Olalekan and Temitope (2021) employed DOI to examine mobile banking adoption in Nigeria, identifying trialability and observability as critical determinants. However, DOI Theory has faced criticism. Greenhalgh et al. (2020) argued that the theory often oversimplifies the complex, context-specific processes of innovation diffusion, focusing predominantly on individual adopters while neglecting organizational and systemic factors. Critics also highlight that DOI assumes a uniform progression through adoption stages, which may not account for barriers like socioeconomic constraints or cultural resistance.

In this study, DOI Theory is relevant in understanding the adoption and implementation of the Central Bank of Kenya (CBK) guidelines among commercial banks. Through a thorough

examination on how attributes such as relative advantage like enhanced online banking security and compatibility issues such as alignment with existing banking systems influence adoption, the theory provides a structured framework for analyzing stakeholder responses. Furthermore, DOI helps identify adopter categories within the banking sector, facilitating targeted strategies to encourage compliance and effective implementation of the CBK guidelines. Therefore, the DOI Theory aids in understanding how innovations like these guidelines spread across Kenya's financial ecosystem.

In this study, DOI Theory is relevant in providing a structured framework for analyzing how these attributes and categories influence the effectiveness of the GCPSP. Through a thorough examination on how attributes such as relative advantage like enhanced online banking security and compatibility issues such as alignment with existing banking systems influence adoption, the theory helped to assess whether the regulations achieve their intended impact and how widely they are adopted across the sector. Furthermore, DOI helped to identify banks based on their adoption patterns facilitating targeted strategies to encourage compliance and effective implementation of the GCPSP.

2.2.3 Agency Theory

Agency Theory, first introduced by Michael C. Jensen and William H. Meckling in 1976 (Jensen & Meckling, 1976).The theory explores the dynamics between principals (those who delegate authority) and agents (those who act on behalf of the principals). It particularly lays emphasis on the conflicts that occur when when ownership and control are separated within organizations (Jensen & Meckling, 1976). The theory proposes that agents, who operate on behalf of principals, might pursue their own interests over the interests of the principals. This can result in agency issues like moral hazard and adverse selection (Fama, 1980). To mitigate these conflicts, principals often implement mechanisms such as contracts, performance incentives and monitoring systems to make sure agents act in the principals' best interests (Eisenhardt, 1989). Agency Theory's focus on information asymmetry and the conflict between self-interest and organizational goals provides a lens for understanding various governance issues, including financial management and risk management (Jensen & Meckling, 1976; Eisenhardt, 1989).

In this scenario, the CBK (as the principal) delegates responsibility to commercial banks (the agents) to ensure secure online transactions (Mutuku, 2020). Commercial banks, acting as agents, may have competing interests such as profit maximization, cost reduction and customer satisfaction, which could lead to conflicting priorities regarding the implementation of the GCPSP (Wanjiru, 2020). According to Agency Theory, these competing interests may result in a failure to fully comply with regulatory requirements, especially when the banks do not face adequate monitoring or enforcement mechanisms (Eisenhardt, 1989). This study analyzed how mechanisms such as incentives, contracts and regulatory frameworks influence commercial banks' adherence to the GCPSP (Mutuku, 2020). Additionally, Agency Theory can help explain the role of the oversight body in ensuring that the actions of commercial banks align with the principal's interests of ensuring secure online transactions (Wanjiru, 2020). The theory highlights the importance of establishing effective monitoring and enforcement mechanisms to address agency problems and enhance compliance with the GCPSP.

2.3 Empirical Literature Review

The empirical literature review discussed the key aspects of the GCPSP implementation, highlighting their impact on online banking.

2.3.1 Access Control Measures and Secure Online Banking Transactions

The empirical gap in the adoption of advanced access control systems in financial institutions can be understood through diffusion theory. Access control innovations, such as multi-factor authentication and biometric security, spread through a process outlined in Rogers' theory, which includes stages like knowledge, persuasion, decision, implementation, and confirmation. However, there is a gap in real-world data on how these systems are adopted and their effectiveness in different institutional contexts. This lack of evidence affects the persuasion and decision stages, as institutions may be hesitant to adopt these technologies without clear, empirical data on their benefits and cost-effectiveness (Miller, 2020).

Additionally, financial institutions may fall into different adopter categories, such as early adopters and laggards, based on their willingness to embrace innovation. The empirical gap limits the understanding of how quickly these innovations spread within the sector, particularly among the early majority and late majority, who often need proven results before making changes (Patel &

Singh, 2021). Diffusion theory helps highlight the factors affecting adoption, such as perceived advantages, compatibility, and observability, which may be influenced by the lack of sufficient real-world studies. Addressing this empirical gap through further research can support the broader adoption of effective access control systems in financial institutions. In the context of Kenya, the adoption of access control measures has seen rapid growth, driven by the increasing use of mobile and internet banking services across urban and rural areas. The Central Bank of Kenya (CBK) has is fundamental in regulating and guiding the implementation of these measures through the introduction of the GCPSP for financial institutions (Mutua & Njoroge, 2020). For instance, banks in Kenya are required to adopt secure access controls like multi-factor authentication and biometric verification to ensure that online banking platforms remain secure (Njoroge, 2021). However, despite these efforts, challenges persist, particularly in rural set ups where accessibility to advanced security infrastructure and financial literacy, which hampers the effective adoption and implementation of these measures is limited (Kinyua, 2020). Additionally, while mobile banking security is improving, there are still cases of cyber fraud that highlight the need for stronger enforcement and constant upgrades of access control systems (Kagiri & Gichuki, 2021). Further research is essential to understand the specific barriers to effective implementation and how access control measures can be optimized in the Kenyan banking context (Kamau, 2021).

2.3.2 Incidence Response and Secure Online Banking Transactions

Incident response refers to the systematic approach organizations take to manage and recover from disruptions caused by cyber incidents, ultimately enhancing cyber resilience (CBK, 2019). In the financial sector, where cyber-attacks such as data breaches, identity theft, and financial fraud are frequent and increasingly sophisticated, banks are under pressure to establish effective incident response plans (Juma, 2021). These plans enable banks to swiftly identify and respond to threats, minimizing their impact on the organization and customers, while also maintaining business continuity and customer trust (Mugo & Njoroge, 2021).

From the perspective of diffusion theory, the adoption of effective incident response strategies follows a process of innovation spread. Diffusion theory outlines how new practices or technologies—such as incident response frameworks—are adopted over time across organizations, influenced by factors such as relative advantage, compatibility, complexity, and observability (Rogers, 2003). As financial institutions adopt incident response mechanisms, the speed and

breadth of adoption are impacted by the perceived benefits (e.g., minimizing disruptions and maintaining customer trust) and the ability to integrate these frameworks into existing systems (Mugo & Njoroge, 2021). Early adopters, such as larger or more technologically advanced banks, lead the way in implementing these practices, while others may follow once the advantages become more visible. The empirical gap in understanding the pace and drivers of adoption of incident response strategies in banks highlights the need for more research on how these strategies spread within the financial sector and how they are tailored to meet the evolving cyber threat landscape. The importance of incident response mechanisms has been emphasized in recent studies from various regions. A Kenyan study by Wambua (2021) found that financial institutions with well-established incident response strategies were more likely to stop or reduce the damage caused by cyber-attacks. These banks were able to maintain a strong customer base and protect their financial assets, underscoring the critical role of preparedness in securing online banking services. A similar study in Europe by Tessema *et al.* (2020) highlights the value of integrating automation and real-time monitoring tools in incident response systems. By leveraging cutting-edge technologies such as machine learning algorithms and AI based detection systems, banks can identify security threats early and respond in real-time, thereby minimizing the risk of fraud and unauthorized transactions. In Asia, Lee (2021) showed that banks utilizing AI in their incident response frameworks had a higher success rate in identifying and mitigating threats compared to those relying solely on manual processes. The integration of AI, coupled with real-time threat monitoring, provides banks with a dynamic approach to addressing evolving cyber risks in an increasingly digital banking environment.

2.3.3 Data Protection Protocols and Secure Online Banking Transactions

Data protection protocols are essential in safeguarding sensitive customer information within online banking systems, ensuring the confidentiality, integrity, and availability of data (Chung, 2020). These protocols involve strategies, technologies, and practices that financial institutions use to protect data during transmission and storage, including encryption techniques, secure communication channels, and multi-factor authentication systems to prevent unauthorized access and data breaches (Ngugi, 2021). Strong data protection measures are critical in online banking, where cyberattacks and identity theft pose heightened risks (Mugambi, 2021). Adherence to international standards, such as GDPR, also ensures compliance with regulations and builds

customer trust (Schmidt et al., 2021). A failure to secure customer data can result in financial losses, regulatory fines, and reputational damage (Mugambi, 2021).

From the perspective of agency theory, financial institutions (principals) delegate the responsibility of securing customer data to their IT teams or third-party service providers (agents). Agency theory highlights potential conflicts of interest, as agents may prioritize their own objectives, such as reducing costs or operational burdens, over the institution's interests in protecting customer data (Lee & Cho, 2020). The empirical gap exists in understanding how effectively principals ensure that agents adhere to data protection protocols. A lack of research on how banks align incentives, monitor agent performance, and ensure compliance with security measures creates uncertainty about the effectiveness of these protections. This gap can hinder the development of more effective governance models to ensure data protection in online banking. Globally, the importance of robust data protection protocols has been highlighted in several studies. In Europe, a study by Schmidt *et al.* (2021) found that banks that implemented advanced encryption and tokenization techniques significantly reduced the risks associated with online banking transactions, particularly in preventing unauthorized data access. Similarly, a study by Anderson (2020) in the US highlights the importance of adopting multi-layered data protection strategies, where banks implement firewalls, encryption and user authentication processes to secure online platforms from cyber threats. These measures have proven effective in mitigating the risk of data breaches, fraud and identity theft, which are prevalent in the digital financial landscape (Anderson, 2020). Additionally, research conducted by Tan *et al.* (2020) in Southeast Asia found that financial institutions that prioritized data protection, alongside continuous monitoring and incident response systems, showed greater resilience against cyber-attacks, further emphasizing the global trend towards prioritizing data security in banking (Tan et al., 2020).

2.3.4 Network Security Standards and Secure Online Banking Transactions

Network security standards are essential in protecting online banking platforms, ensuring that financial transactions remain secure from cyber threats (Sambasivan & Tan, 2020). These standards include protocols, technologies, and best practices that prevent unauthorized access, ensure data integrity, and create a secure environment for customers (Sambasivan & Tan, 2020). Implementing technologies like firewalls, intrusion detection systems (IDS), and encryption methods helps reduce the risks of cyberattacks, such as phishing, ransomware, and data breaches

(O'Neill, 2021). In the context of agency theory, the relationship between financial institutions (principals) and external security service providers or internal IT departments (agents) highlights the need for aligning interests in ensuring optimal network security.

Agency theory suggests that principals (e.g., banking institutions) may not always directly oversee the actions of their agents (e.g., IT security teams or third-party service providers), which can lead to conflicts of interest or inefficiencies (Lee & Cho, 2020). By adopting robust network security measures, financial institutions mitigate risks and align their agents' actions with their own interests—protecting customer data, assets, and complying with industry regulations. As cyber threats evolve, institutions must ensure their agents update security protocols regularly to address emerging vulnerabilities, thus reducing the potential for agency problems (O'Neill, 2021).In the context of Kenya, research has shown that while larger banks are adopting network security standards, challenges remain for smaller institutions, particularly in terms of resource allocation and technological expertise. A study by Mwangi *et al.* (2021) highlighted that larger bank in Kenya had made significant strides in implementing industry-standard firewalls and intrusion detection systems, but smaller banks faced difficulties due to budget constraints and limited access to advanced security tools. Despite regulatory efforts, such as those of the CBK, gaps remain in the uniform application of network security standards across the banking sector (Mutuku, 2020). The lack of standardized security measures across banks increases the vulnerability of the sector to cyber-attacks. Wakoli (2024) noted that customer awareness of cyber security measures remains low in Kenya, which exacerbates the challenges in ensuring secure online banking transactions.

2.3.5 Institutional Resources

The empirical gap regarding the role of institutional resources in enhancing the effectiveness of cybersecurity measures can be understood through diffusion theory. Institutional resources—financial, human, and technological—are crucial for the successful implementation and maintenance of cybersecurity systems, particularly in banking (Akinmoladun & Adeyemi, 2020). However, there is limited empirical evidence on how these resources specifically influence the adoption of cybersecurity tools within different financial institutions. According to diffusion theory, the adoption of innovations, such as cybersecurity measures, is influenced by the availability of resources and organizational readiness (Wambui & Mwaura, 2021). The empirical

gap exists in understanding how resource constraints or abundance impact the speed and breadth of cybersecurity tool adoption.

Financial institutions with robust institutional resources are better positioned to adopt cutting-edge cybersecurity technologies, yet those with fewer resources may lag behind. This gap affects the persuasion and implementation stages of adoption, as institutions may struggle to deploy or maintain cybersecurity systems without adequate funding, skilled personnel, or technological infrastructure (Mwangi & Kimani, 2021). Diffusion theory highlights that the presence of strong institutional resources can significantly accelerate the adoption of cybersecurity innovations, while their absence can impede progress, ultimately influencing the GCPSP's effectiveness on online banking transactions.Similarly, Wambui and Mwaura (2021) conducted research in Kenya and confirmed that institutional resources were fundamental in the effectiveness of cyber security frameworks in commercial banks. Their study found that larger Kenyan banks, which had more financial resources and access to advanced technologies, were better positioned to implement and adhere to the Central Bank of Kenya's GCPSP (Wambui & Mwaura, 2021). These banks invested heavily in training programs, technological tools and security infrastructure, which enhanced their ability to mitigate risks related to online banking fraud and cybercrime (Wambui & Mwaura, 2021). In contrast, smaller banks with limited institutional resources struggled to keep up with the implementation of the GCPSP, facing challenges such as inadequate funding for cyber security tools and a shortage of qualified personnel (Wambui & Mwaura, 2021). These disparities further illustrate how institutional resources can moderate the effectiveness of cyber security as laid down in the GCPSP, with well-resourced institutions able to fully comply with the CBK's directives, leading to more secure online banking transactions (Mwangi & Kimani, 2021).

In a more recent study, Mwangi and Kimani (2021) explored the longitudinal impact of institutional resources on the effectiveness of the GCPSP in reducing cybercrime. Their study indicated that larger banks in Kenya, which had significant institutional resources, experienced a notable decline in cybercrime incidents after implementing the GCPSP (Mwangi & Kimani, 2021). These banks were able to invest in robust cybersecurity infrastructure and were better able to train their staff in identifying and mitigating cyber threats (Mwangi & Kimani, 2021). Conversely, the study found that smaller banks, especially those located in rural areas, struggled with the enforcement of the GCPSP due to limited access to resources (Mwangi & Kimani, 2021). This

resource gap hindered their ability to keep up with evolving cyber threats, leaving them more vulnerable to online banking fraud (Mwangi & Kimani, 2021). The study highlights the moderating role of institutional resources, indicating that while the GCPSP is crucial in enhancing cybersecurity, the degree to which the GCPSP can be effectively implemented depends heavily on the availability of institutional resources (Wambui & Mwaura, 2021).

Despite the clear role of institutional resources in moderating the impact of the GCPSP, the literature on this subject remains somewhat limited, particularly in addressing how the strategic allocation of these resources can improve cybersecurity outcomes (Akinmoladun & Adeyemi, 2020). Future research could focus on understanding how different types of institutional resources (financial, technological, and human) can be optimized to enhance the success of cybersecurity measures (Mwangi & Kimani, 2021). Additionally, it would be valuable to examine the specific challenges faced by small and medium-sized banks in resource allocation and their capacity to implement the GCPSP effectively (Wambui & Mwaura, 2021). This could help develop tailored strategies for resource-poor institutions, ensuring that all banks, regardless of size, can benefit from improved security measures and reduced vulnerabilities in online banking (Akinmoladun & Adeyemi, 2020).

2.4 Summary of Knowledge Gap

The knowledge gap in evaluating the implementation of the CBK's Guideline on GCPSP and its impact on secure online banking transactions lies in the limited understanding of how effectively the GCPSP is being enforced across the diverse range of commercial banks in Kenya. While the CBK has introduced comprehensive regulations aimed at improving online banking security, there is a lack of in-depth studies examining the practical implementation challenges faced by banks, especially smaller and rural-based institutions (Mutuku, 2020). Moreover, while previous research has explored the importance of cyber security measures in online banking, there is insufficient evidence on the direct correlation between the adoption of the GCPSP and a reduction in cyber security breaches or fraud (Mugambi, 2020). Furthermore, the role of customer awareness, employee training and bank-specific resources in successfully applying the GCPSP remains underexplored. This investigation tries to remedy these gaps by evaluating the effectiveness of the GCPSP in enhancing online banking security and identifying the level of extent to the implementation across the Kenyan banking sector.

TABLE 2. 1: RESEARCH GAPS

Author	Tittle	Methods	Findings	Gaps	Focus
Karanja & Mwai (2020)	Evaluating the Role of Financial Institutions in Addressing Cybersecurity Challenges in Kenya	Quantitative, survey of 30 commercial banks	Identified that financial institutions in Kenya have implemented various cyber security measures, but challenges persist, particularly in resource allocation for cyber security teams	**Conceptual** Focused primarily on financial institutions' efforts and did not explore the customers' role or awareness in improving online banking security	Improving online banking security through CBK guidelines implementation framework
Wambui & Mwaura (2021)	The impact of cyber security risk management strategies on operational efficiency in Kenyan banks	Case study, in-depth interviews with operational managers	Found that banks with robust cyber security frameworks, including adherence to GCPSP, experienced fewer disruptions in online banking services, improving operational efficiency	**Conceptual** Did not analyze the specific challenges smaller banks face in implementing these cyber security frameworks	Implementing the cyber security frameworks on 1st,2nd and 3rd tier banks

Otieno & Kamau (2022)	Investigating the relationship between cyber security, the GCPSP and financial loss prevention in Kenyan banks	Mixed-methods, data analysis of financial loss records from 10 banks	Established that the GCPSP has contributed to a reduction in financial losses related to online banking fraud, with a stronger impact in larger banks	**Conceptual** Did not address the overall public perception of security improvements post-implementation	Educating the bank workforce on security improvements post-implementation framework of CBK
Mutiso & Kipkemboi (2021)	Cyber security risks and financial implications in Kenya's digital banking landscape	Mixed-methods, financial data analysis and interviews with bank executives	Found that cyber security risks lead to significant financial losses in Kenyan banks, with more severe consequences for smaller banks	**Conceptual** Did not explore customer views on compensation and transparency when affected by cyber incidents.	Addressing the cyber incidents framework
Kirui & Gikaru (2020)	Barriers to effective implementation of cyber security laid down in the GCPSP in Kenyan Commercial Banks	Qualitative, interviews with 30 bank officials	Identified resource constraints, lack of skilled personnel, and resistance to change as major barriers to implementing the GCPSP effectively	**Methodological** Did not provide specific strategies for overcoming the challenges faced by smaller banks in resource allocation	Addressing recommendation of overcoming challenges of CBK implementation framework of 3rd tier banks
Mwangi & Kimani (2021)	The effectiveness of Central	Longitudinal study, analyzing	Found a steady decline in cybercrime	**Methodological** Lacked consideration of	Strengthening Cyber security

	bank of Kenya GCPSP in reducing cyber security threats in financial institutions	data from banking institutions over five years	incidents after the implementation of the GCPSP, especially in larger banks with advanced technological infrastructure	rural banks or the impact of technology on cybercriminal activities in Kenya	policies in Banks
Kamau & Limo (2021)	Impact of Cyber security frameworks on financial Data protection in Kenyan online banking	Quantitative, survey of 15 banks and 400 customers	Concluded that data protection frameworks in compliance with the GCPSP have significantly reduced incidents of financial data breaches.	**Methodological** Did not address consumer awareness programs or the role of third-party cyber security audits in enhancing data protection.	Regulating access controls in the 1st 2nd and 3rd tier banks

2.5 Conceptual Framework

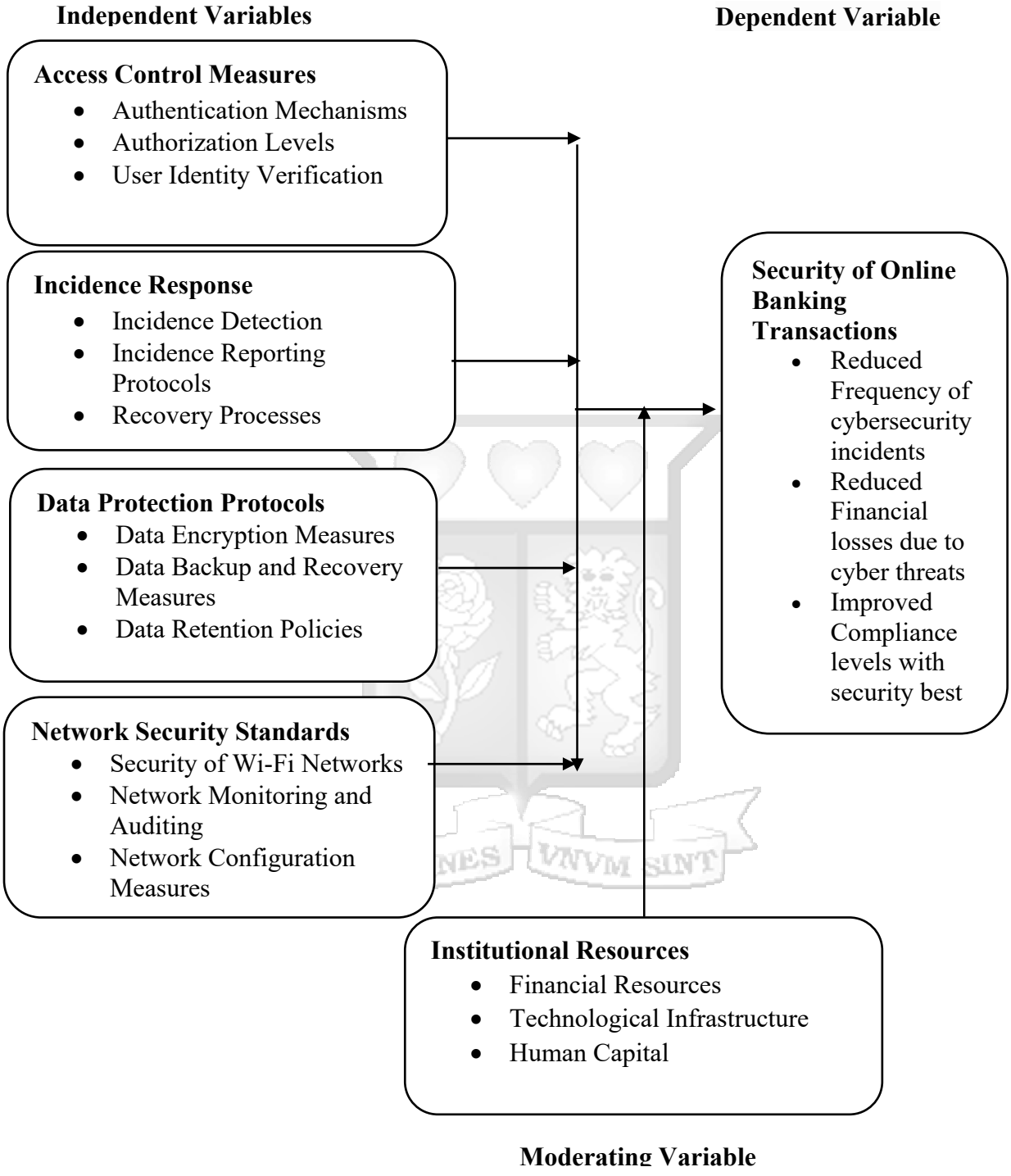


FIGURE 2. 2: CONCEPTUAL FRAMEWORK

2.6 Operationalization of Study Variables

TABLE 2. 2: OPERATIONALIZATION OF STUDY VARIABLES

Variable	Construct	Definition	Indicators	Measurement	Supporting Literature
Access Control Measures	Control Systems for System Access	Systems and policies that ensure only authorized users can access online banking platforms, ensuring confidentiality and protection of data	Authentication Mechanisms Authorization Levels User Identity Verification	Questionnaire: Likert scale questions on the frequency and effectiveness of access control measures	Alsadi, N. et al. (2020); Onwuchekwa, S. & George, J. (2021); Kamau, R. & Limo, S. (2021)
Incidence Response	Response to Security Breaches	Measures taken to address and mitigate the effects of cyber security incidents, including fraud, hacking and data breaches	Incidence Detection Incidence Reporting Protocols Recovery Processes	Questionnaire: Likert scale questions on the effectiveness of incident response strategies	Mwai & Wambui (2021); Kirui & Gikaru (2020); Kamau & Limo (2021)
Data Protection Protocols	Safeguarding Sensitive Information	Protocols that ensure customer data, especially	Data Encryption Measures	Questionnaire: Likert scale questions on data	Anderson, J(2020)

		sensitive information, is safely kept and transmitted to avoid loss or unauthorized access.	Data Backup and Recovery Measures Data Retention Policies	encryption and storage practices and Frequency of data access audits	
Network Security Standards	Safeguarding Network Infrastructure	GCPSP and measures to protect the bank's network infrastructure from external and internal cyber security threats, such as malware or hacking	Security of Wi-Fi Networks Network Monitoring and Auditing Network Configuration Measures	Questionnaire: Likert scale questions on the implementation of firewalls and intrusion detection systems	Otieno & Kamau (2022); Wambui & Mwaura (2021); Mwangi & Kimani (2021)
Institution-al Resources	Organization-al Support Systems	The deployment of human, financial and technological resources within a bank to implement and maintain cyber security measures effectively.	Financial Resources Technological Infrastructure Human Capital	Questionnaire: Likert scale questions on the availability of cyber security budget and framework	Kirui & Gikaru (2020); Wambui & Mwaura (2021); Kamau & Limo (2021)

Secure Online Banking Trans-actions	Secure Transactions in Online Banking	The ability to execute online banking transactions with protection against fraud, data breaches and unauthorized access.	Frequency of cybersecurity incidents Financial losses due to cyber threats Compliance levels with security best practices	Questionnaire: Likert scale questions on transaction security measures (encryption, authentication) and Frequency of fraud detection during transactions	Mwangi & Kimani (2021); Mutiso & Kipkemboi (2021); Karanja & Mwai (2020)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the approach adopted to address the research objectives comprehensively. It details the research philosophy and design, the target population, sampling procedures, data collection methods and tools, as well as data analysis techniques used to achieve reliable and valid findings

3.2 Research Philosophy

Research philosophy is the foundational belief system that shapes how researchers approach studying a phenomenon (Mackenzie & Knipe, 2006). The positivist philosophy holds that there is a single, objective reality that can be measured and understood through sensory experiences. It emphasizes quantitative methods to test hypotheses and uncover truths about the world (Creswell & Creswell, 2017). In contrast, interpretivism suggests that reality is subjective and constructed through human experiences, making qualitative methods more suitable for understanding meaning and context. Interpretivists argue that knowledge is created through social interactions and cultural contexts (Creswell & Creswell, 2017). Pragmatism focuses on practical outcomes and solutions, blending both qualitative and quantitative approaches depending on the research question. Pragmatists believe that truth is not absolute but is determined by what works best in specific contexts, and they prioritize addressing real-world problems (Bryman, 2016). For this study, positivism was chosen as the philosophical assumption, as it aligns with the belief that knowledge can be gained from observable, measurable phenomena and that scientific methods provide objective insights into reality (Creswell & Creswell, 2017).

3.3 Research Design

Research design refers to the strategy employed by a researcher to structure, collect, analyze, and interpret data in a study (Saunders et al., 2019). This study adopts a descriptive survey research design, which provides a detailed account of a phenomenon as it naturally occurs, without manipulating variables (Saunders et al., 2019). However, incorporating correlational research would enhance the study by exploring relationships between variables, offering a deeper understanding. Gathering insights from 11 different bank officials, rather than just one senior

official, ensures a broader and more comprehensive perspective, uncovering diverse viewpoints, reducing bias, and providing a clearer overall picture (Saunders et al., 2019).

3.4 Target Population

The target population comprised of a sample of participants or individuals with specific attributes of interest and are relevant to a study (Asiamah, Mensah, and Oteng-Abayie, 2017). In this investigation, the target population constituted of all commercial banks in Kenya. Data obtained from the CBK indicates that there are 38 commercial banks and 1 mortgage finance company, which has transitioned to provide commercial banking services, in the country.

The population is tabulated as in the table below;

TABLE 3. 1: TARGET POPULATION

Population Characteristic	**Number of Individuals**
Chief Executive Officer	39
General Manager	39
Operations Manager	39
Chief Technology Officer	39
Human Resource Manager	39
Risk Officer	39
Chief Financial Officer,	39
Chief Research and Development Officer	39
Chief Credit Officer	39
Shared services Manager	39
Chief ICT Officer	39
Total	**429**

3.5 Sample Size and Sampling Technique

3.5.1 Sampling Technique

In research study, a sampling technique involves selecting a smaller group of individuals, items, or observations from a larger population to represent that entire group (Creswell & Creswell, 2017). It is essential for obtaining data that is both manageable and statistically valid, ensuring that the conclusions drawn from the sample can be generalized to the larger population (Flick, 2020). A sample is a group of individuals or elements chosen from a larger population, meant to represent that population in a research study. Sampling is conducted to gather data that is manageable, cost-effective and statistically valid, without needing to survey the entire population (Creswell & Poth, 2021).

The sample determination proceeded with the Taro Yamane (Yamane, 1967) formula, at 95% confidence level.

The calculation of sample size was presented as follows.

$$n = \frac{N}{1+N(e)^2}$$

Where;

n= Sample Size

N= Target Population

e= Error Margin

Therefore;

$$n = \frac{429}{1+429\ (0.05)^2} = 220$$

Appling the formula above, the sample size of the research was 220 respondents.

This implies that out of the total population (429 management personnel), only 220 participated in the study. This implied that each stratum contributed 20 individuals to the sample, ensuring proportional representation across all roles. This means that 20 banks were reached out for the study, which were subdivided into tier 1 banks, tier 2 banks and tire 3 banks. The researcher selected them randomly, such that each bank gets an equal opportunity to participate. The sample size was presented as below:

TABLE 3. 2: SAMPLE SIZE

Population Characteristic	**Population**	**Sample Size**
Chief Executive Officer	39	20
General Manager	39	20
Operations Manager	39	20
Chief Technology Officer	39	20
Human Resource Manager	39	20
Risk Officer	39	20
Chief Financial Officer,	39	20
Chief Research and Development Officer	39	20
Chief Credit Officer	39	20
Shared services Manager	39	20
Chief ICT Officer	39	20
Total	**429**	**220**

The views of a variety of officials in the targeted banks were sought so that a more comprehensive interpretation of each of the matters to be addressed is obtained. While the view of a single participant could provide valuable perceptions, multiple viewpoints will uncover different features, potential biases and substitute reasons for a particular matter. Diverse points of view will provide a clearer picture that a single perspective alone.

3.6 Data Collection Method

Data collection methods involved systematic procedures used to gather information required to meet the study's objectives. In our context, data on the implementation of Central Bank of Kenya GCPSP and the security of online transactions was collected from commercial banks in the country. A questionnaire was the primary data collection instrument, as it is an effective tool for obtaining structured responses from a large sample in a standardized manner (Flick, 2020). The questionnaire included a 5-point Likert scale to measure respondents' perceptions and attitudes toward the implementation of CBK GCPSP and their impact on online transaction security. The Likert scale is widely used for assessing levels of agreement or disagreement with given statements, making it ideal for capturing detailed insights into the study's focus areas (Fink, 2019). Response options ranged from "Strongly Disagree" to "Strongly Agree," enabling a comprehensive analysis of participants' views.

3.7 Research Quality

Ensuring high-quality research involves the systematic application of measures to increase the reliability, validity and rigor of the investigation. Research quality is critical to achieving credible, accurate and meaningful results that contribute to academic and practical knowledge. In this study, which focused on the adoption of the GCPSP and the security of online transactions in commercial banks in Kenya, research quality was addressed through piloting and testing for reliability and validity.

3.7.1 Piloting

Piloting is a crucial step in ensuring the reliability and validity of the research instruments. It involves testing the questionnaire on a smaller, selected sample before the main data collection phase begins. In this study, approximately 10% of the total sample size, which equated to 22 respondents, participated in the pilot phase. Piloting in this study allowed the researcher to identify any flaws or ambiguities in the instrument, making sure all questions are clear, understandable and relevant to the study's objectives. Feedback from these pilot respondents was invaluable in refining the questionnaire, helping to eliminate any misunderstandings or errors in the phrasing of the questions. This process allowed for fine-tuning of the instrument, ensuring that it effectively captures valid and reliable data during the main data collection phase. Furthermore, piloting

provided an opportunity to assess the time taken to complete the questionnaire, ensuring that it is reasonable for the respondents.

3.7.2 Reliability

Reliability denotes the consistency of the research instruments in yielding the same results when applied under similar conditions (Creswell & Creswell, 2017). To ensure reliability, the questionnaire used in this study underwent a pilot test with a small sample of respondents from the target population but not included in the main study. The results of the pilot test were analyzed to refine and adjust the questions, ensuring clarity and consistency in the instrument's application. Cronbach's alpha coefficient was used to assess the internal consistency of the Likert scale items, with a threshold of 0.7 or higher considered acceptable for reliability (Saunders *et al.,* 2019).

3.7.3 Validity

In this study, validity refers to how well the research instrument measures what it is supposed to measure (Kothari, 2009). This study incorporated content validity and construct validity to enhance the research quality. Content validity was guaranteed through the questionnaire which was developed in alignment with the study's objectives and submitted to the supervisor for review. Construct validity was realized through aligning the questions with the theoretical framework and key variables, such as the GCPSP and online transaction security, to ensure they accurately capture the constructs under investigation.

3.8 Data Analysis and Presentation

The procedure for data analysis entail packaging of information gathered, assembling and marshaling its core components in a manner that the findings can be passed on easily and effectively (Cameron, Sankaran & Scales, 2015). Descriptive and inferential statistics were used in carrying out analysis of data gathered for this research. The projected also tested diagnostic test for the variables.

3.9 Ethical Considerations

The study maintained ethical standards by ensuring voluntary participation throughout the research process. Participants were informed of the potential positive and negative consequences of their involvement, enabling them to make a well-informed choice regarding their involvement. The data was collected between February and April 2025. When seeking consent, the researcher provided a clear explanation of the purpose of the research and its relevance to the selected field, ensuring

transparency. Additionally, the researcher maintained the integrity of the study by ensuring that no irrelevant, imaginary, or fictitious data is used in the analysis. Only authentic and accurate data was considered for analysis, guaranteeing that the findings are based on legitimate responses and observations. The researcher also refrained from using data from previous studies to ensure that the results are original and contribute to the current research gap. Consent was obtained from all participating commercial banks, ensuring that the institutions are fully informed of the research objectives and processes. Informed consent was also sought from individual respondents, ensuring their understanding of their rights and the study's purpose.

3.10 Chapter Summary

This chapter outlined the research methodology for the study, detailing the approach and strategies that were employed to collect and analyze data. The research philosophy underpinning this study was positivism, which emphasizes objective, observable, and measurable data, aligning with the quantitative nature of the study. The research design, informed by the study objectives was structured to provide comprehensive insights into the implementation of CBK guidelines and the security of online transactions in commercial banks in Kenya. The chapter showed that the study adopts a descriptive survey research design, with the population consisting of key management personnel from various commercial banks in Kenya. A sample size of 220 respondents was selected using a stratified random sampling technique. Data was collected using a structured questionnaire, which included Likert scale items to measure respondents' attitudes toward security measures and the implementation of CBK guidelines. Piloting of the questionnaire was conducted with a smaller sample size to ensure its reliability and validity before the main data collection. In the chapter, it was shown that data was analyzed using descriptive statistics through SPSS Version 22.0, focusing on percentages, means, and standard deviations to summarize and interpret the data. Ethical considerations, including informed consent from participants and institutions, were strictly followed. The study ensured the integrity of the data by avoiding the use of fictitious or irrelevant data. Finally, the chapter detailed how consent was sought from the commercial banks, individual respondents, the University, and NACOSTI to ensure full compliance with ethical and regulatory standards.

CHAPTER FOUR

PRESENTATION OF FINDINGS

4.1 Introduction

This chapter presents the analysis and interpretation of the data collected in relation to the objectives of the study. The purpose of this chapter was to examine the patterns, trends, and relationships derived from the responses of the study participants. The data was analyzed using quantitative techniques, with the aid of the statistical package for social sciences to generate descriptive and inferential statistics. Tables, charts, and graphs were employed to enhance the clarity and visualization of the results. The findings were presented in a structured manner, beginning with the demographic characteristics of the respondents, followed by an analysis of each research variable. The results are then interpreted in light of the research questions and objectives, providing the foundation for the discussion in the subsequent chapter.

4.2 Response Rate

The study targeted a total of 220 respondents, out of which 194 successfully participated in the research by completing and returning the questionnaires. This represents a response rate of 88.2%, which is considered excellent for purposes of data analysis and drawing meaningful conclusions. As noted by Mugenda and Mugenda (2003), a response rate of 50% is adequate, 60% is good, and a rate above 70% is very good. Therefore, the response rate of 88.2% indicates a high level of cooperation among the targeted participants and enhances the reliability and validity of the data gathered for this study.

The summary of the response rate is presented in Table 4.1 below:

TABLE 4. 1: RESPONSE RATE

Category	Frequency	Percentage (%)
Responded	194	88.2%
Did not Respond	26	11.8%
Total	**220**	**100%**

4.3 Reliability Analysis

To assess the internal consistency of the research instrument, a reliability analysis was conducted using Cronbach's Alpha coefficient. This statistical measure determines the degree to which items within a construct are interrelated, reflecting the reliability of the scale. According to Mugenda and Mugenda (2003) and Gliem and Gliem (2003), a Cronbach's Alpha value of 0.700 and above is considered acceptable, 0.800–0.899 is deemed good, and 0.900 and above indicates excellent reliability. The study focused on six constructs, comprising of four independent variables including; Access Control Measures, Incidence Response, Data Protection Protocols, and Network Security Standards; one mediating variable which was Institutional Resources; and a dependent variable, which was Security of Online Banking Transactions. Each construct was measured using multiple items, and their internal consistency was assessed.

The reliability results showed that access control measures had a cronbach's alpha value of 0.901, data protection protocols scored 0.912, and network security standards recorded 0.917, all indicating excellent internal consistency. Incidence response had a cronbach's alpha of 0.879, institutional resources scored 0.886, and security of online banking transactions yielded 0.895, all of which indicate good reliability. The average Cronbach's Alpha of 0.898, which falls within the good reliability range, confirming that the overall research instrument is highly reliable for measuring the constructs. Therefore, all constructs showed Cronbach's Alpha values exceeding the minimum threshold of 0.700. The average Cronbach's Alpha value of 0.898 supports the internal consistency of the instrument and the reliability of the collected data.

TABLE 4. 2: RELIABILITY STATISTICS

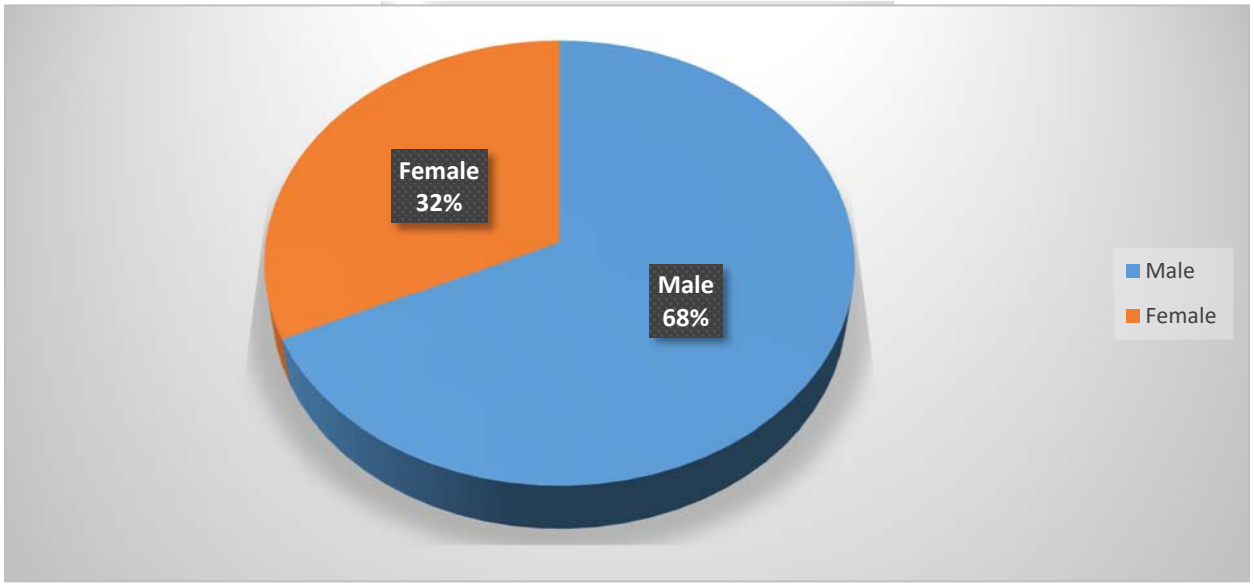
Construct	Category	Number of Items	Cronbach's Alpha	Reliability Level
Access Control Measures	Independent Variable	7	0.901	Excellent
Incidence Response	Independent Variable	7	0.879	Good
Data Protection Protocols	Independent Variable	7	0.912	Excellent
Network Security Standards	Independent Variable	7	0.917	Excellent
Institutional Resources	Mediating Variable	7	0.886	Good

Construct	Category	Number of Items	Cronbach's Alpha	Reliability Level
Security of Online Banking Transactions	Dependent Variable	7	0.895	Good
Average		7	**0.898**	Good

4.4 Demographic Information Results

4.4.1 Gender

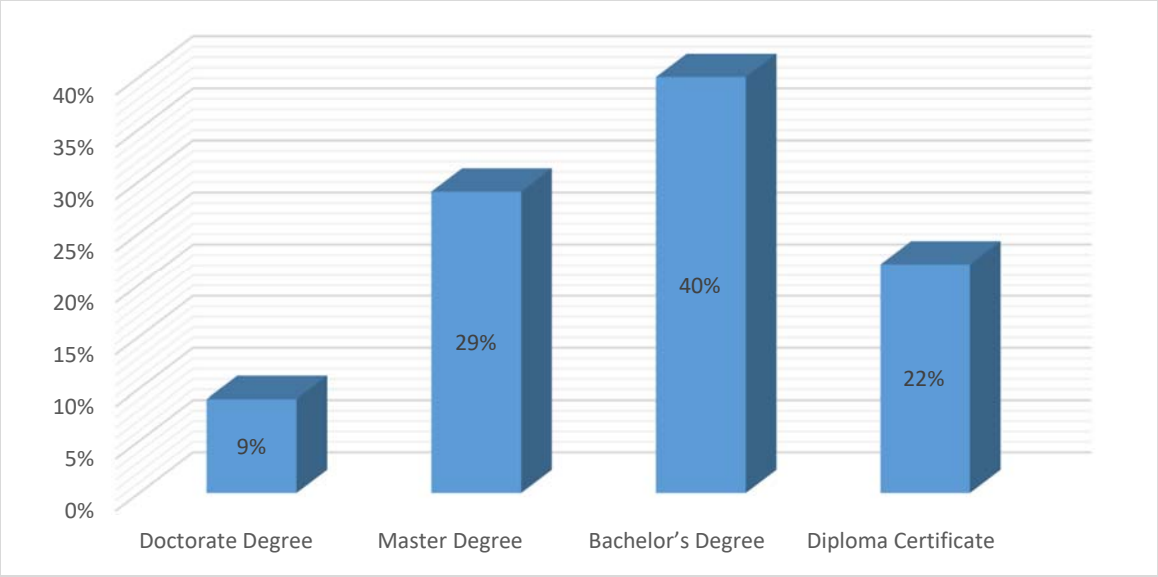
The study sought to establish the gender of the respondents. The findings were presented in the figure below;



The study results showed that a majority of the respondents (68%) were male, with females making up 32% of the total sample. These findings imply that at the time the study was being conducted, most of the respondents reached were male.

4.4.2 Highest Level of Education

The study sought to establish the highest level of education of the respondents. The findings of the study were presented in the figure below;



From the findings of the study, it was evident that a significant portion (40%) of the sample holds a Bachelor's Degree, followed by those with Master's Degrees (29%). Diploma Certificates account for 22%, while only 9% of respondents hold a Doctorate Degree. This suggests that the sample is relatively highly educated, with most respondents having completed undergraduate or postgraduate studies.

4.4.3 Professional Certification and Experience

The study sought to establish the professional qualification of the respondents. The findings were presented in the table below;

	Certification	**Frequency**	**Percentage (%)**
Professional Certification	CFE	22	11.3
	CFA	18	9.3
	CPA	62	31.9
	ACCA	35	18.0
	Experience Range	**Frequency**	**Percentage (%)**
Professional Experience	1–5 Years	48	24.7
	6–10 Years	67	34.5
	11–15 Years	35	18.0
	16–20 Years	32	16.5
	Over 20 Years	12	6.2

From the findings of the study, it was evident that the most common certification held by respondents was CPA (31.9%), followed by ACCA (18.0%) and CFE (11.3%). A smaller portion of respondents (9.3%) have the CFA certification. This distribution indicates that while a large group of respondents have accounting and finance-related certifications, there is also a diverse set of professionals, with varying qualifications. The presence of certifications like CPA and ACCA suggests a sample of individuals working in accounting, finance, or auditing roles, while the smaller number of CFA holders could point to those in investment or financial analysis fields.

The table also summarizes the Years of Professional Experience and shows that the largest group of respondents (34.5%) have between 6–10 years of experience, followed by those with 1–5 years (24.7%). 11–15 years of experience account for 18%, while 16.5% have 16–20 years of experience, and 6.2% have more than 20 years of professional experience. This indicates a relatively even distribution of experience levels across the sample, with a concentration in the mid-career range (6-10 years).

4.5 Access Control Measures and Security of Online Banking Transactions

The study aimed to assess respondents' perceptions regarding the effectiveness of access control measures and their influence on the security of online banking transactions. The findings of the study are summarized in the table below;

TABLE 4. 3: ACCESS CONTROL AND SECURITY OF ONLINE BANKING TRANSACTIONS

Statement	Mean	Standard Deviation
The security measures in place provide strong protection for online banking transactions	4.271	0.683
I feel that access control measures effectively prevent unauthorized access to online banking accounts	4.193	0.721
My confidence in the security of online banking transactions is high due to the controls my bank has implemented	4.106	0.755
Security controls in my bank are reliable and reduce the likelihood of fraud in online banking	4.158	0.792

Statement	Mean	Standard Deviation
The bank's access control systems make customers feel safe when performing online transactions	4.239	0.704
Access control measures in online banking are user-friendly and do not create unnecessary difficulties for customers	3.874	0.823
The bank's security measures provide comprehensive protection for clients' personal and financial information	4.216	0.741
Overall Mean	**4.151**	

From the analyzed data, the findings of the study showed that a majority of the respondents agreed that the security measures in place provide strong protection for online banking transactions, as shown by a mean of 4.271 (Std Dev=0.683). In addition, the results of the study showed that a majority of the respondents indicated their agreement with the statement that access control measures effectively prevent unauthorized access to online banking accounts, as shown by a mean of 4.193 (Std Dev = 0.721). also, the findings of the study further showed that a majority of the respondents agreed that their confidence in the security of online banking transactions is high due to the controls their bank has implemented, as shown by a mean of 4.106 (Std Dev = 0.755). In addition, the results indicated that a majority of the respondents agreed that security controls in their bank are reliable and reduce the likelihood of fraud in online banking, as shown by a mean of 4.158 (Std Dev = 0.792).

Further, the study findings also revealed that a majority of the respondents agreed that the bank's access control systems make customers feel safe when performing online transactions, as shown by a mean of 4.239 (Std Dev = 0.704). In addition, the findings of the study showed that a majority of the respondents agreed that access control measures in online banking are user-friendly and do not create unnecessary difficulties for customers, as shown by a mean of 3.874 (Std Dev = 0.823). As well, the results of the study showed that a majority of the respondents agreed that the bank's security measures provide comprehensive protection for clients' personal and financial information, as shown by a mean of 4.216 (Std Dev = 0.741). The overall mean stood at 4.151, indicating general agreement among the respondents across all statements. These findings concur

with a study conducted by Al-Emran, Shaalan, and Al-Kabi (2020), which showed that users' trust in online banking platforms is significantly influenced by robust access control systems, user-friendly security features, and the perception of comprehensive protection of personal and financial data. Their research emphasized that effective security practices enhance users' confidence and willingness to adopt and rely on digital banking services.

4.6 Incidence Response and Security of Online Banking Transactions

The study sought to determine the level of agreement among respondents regarding the effectiveness of incident response mechanisms in enhancing the security of online banking transactions in Kenya's commercial banks. The findings of the study were presented in the table below;

TABLE 4. 4: INCIDENT RESPONSE AND SECURITY OF ONLINE BANKING TRANSACTIONS

Statement	Mean	Std Dev
1. Our bank has a well-defined incident response plan for online banking security breaches.	4.187	0.791
2. The incident response procedures are regularly tested and updated to handle new security threats.	4.124	0.829
3. Online banking security breaches are effectively managed and mitigated by the bank.	4.068	0.877
4. The bank ensures prompt communication with customers in case of a security incident.	4.014	0.915
5. I feel confident that online banking transactions are secure due to the incident response plan.	4.102	0.841
6. The bank's online banking platform is regularly tested for vulnerabilities.	3.961	0.934
7. Our bank conducts regular post-incident reviews to improve future response strategies.	3.998	0.902
Overall Mean	**4.065**	

The findings of the study showed that a majority of the respondents agreed that their bank has a well-defined incident response plan for online banking security breaches, as shown by a mean of 4.187 (Std Dev = 0.791). In addition, the results of the study showed that a majority of the respondents indicated their agreement with the statement that the incident response procedures are regularly tested and updated to handle new security threats, as shown by a mean of 4.124 (Std Dev = 0.829). The study findings further showed that a majority of the respondents agreed that online banking security breaches are effectively managed and mitigated by the bank, as shown by a mean of 4.068 (Std Dev = 0.877). In addition, a majority of the respondents indicated their agreement with the statement that the bank ensures prompt communication with customers in case of a security incident, as shown by a mean of 4.014 (Std Dev = 0.915).

The results of the study also showed that a majority of the respondents agreed that they feel confident that online banking transactions are secure due to the incident response plan, as shown by a mean of 4.102 (Std Dev = 0.841). Further, the findings revealed that a majority of the respondents agreed that the bank's online banking platform is regularly tested for vulnerabilities, as shown by a mean of 3.961 (Std Dev = 0.934). Also, the study found that a majority of the respondents agreed that their bank conducts regular post-incident reviews to improve future response strategies, as shown by a mean of 3.998 (Std Dev = 0.902). The overall mean stood at 4.065, indicating that, on average, the respondents agreed with the statements relating to the role of incident response in securing online banking transactions. These findings concur with the study done by Akhter and Sultana (2020), which showed that incident response planning, real-time monitoring, and post-event assessments significantly improve customer trust and reduce the risk of repeated breaches in digital banking environments.

4.7 Data Protection Protocols and Security of Online Banking Transactions

The study sought to determine the level of agreement among respondents concerning the effect of data protection and encryption protocol measures on the security of online banking transactions in commercial banks in Kenya. The results are presented in the table below.

TABLE 4. 5: DATA PROTECTION AND ENCRYPTION PROTOCOLS

Statement	Mean	Std Dev
1. The data protection policies in place effectively safeguard customer information.	4.139	0.826
2. The encryption protocols used by our bank adequately protect sensitive data from unauthorized access.	4.127	0.837
3. Our systems prevent data breaches and protect customer data effectively.	4.078	0.873
4. Staff training on data protection and encryption protocols is sufficient for us to handle sensitive information responsibly.	4.042	0.896
5. Our bank regularly updates their data protection and encryption protocols to adapt to emerging threats.	4.065	0.881
6. My bank takes adequate measures to comply with relevant data protection regulations.	4.006	0.929
7. Data protection and encryption measures contribute to customer trust in our banking services.	4.084	0.864
Overall Mean	**4.077**	

The findings of the study showed that a majority of the respondents agreed that the data protection policies in place effectively safeguard customer information, as shown by a mean of 4.139 (Std Dev = 0.826). In addition, the results of the study showed that a majority of the respondents indicated their agreement with the statement that the encryption protocols used by their bank adequately protect sensitive data from unauthorized access, as shown by a mean of 4.127 (Std Dev = 0.837). The study findings further showed that a majority of the respondents agreed that their systems prevent data breaches and protect customer data effectively, as shown by a mean of 4.078 (Std Dev = 0.873). In addition, a majority of the respondents indicated their agreement with the statement that staff training on data protection and encryption protocols is sufficient for them to handle sensitive information responsibly, as shown by a mean of 4.042 (Std Dev = 0.896).

The results of the study also showed that a majority of the respondents agreed that their bank regularly updates their data protection and encryption protocols to adapt to emerging threats, as

shown by a mean of 4.065 (Std Dev = 0.881). Further, the findings revealed that a majority of the respondents agreed that their bank takes adequate measures to comply with relevant data protection regulations, as shown by a mean of 4.006 (Std Dev = 0.929). Lastly, the study found that a majority of the respondents agreed that data protection and encryption measures contribute to customer trust in their banking services, as shown by a mean of 4.084 (Std Dev = 0.864). The overall mean stood at 4.077, indicating that, on average, the respondents agreed with the statements relating to the role of data protection and encryption in safeguarding online banking transactions. These findings concur with the study conducted by Furnell and Shah (2020), which showed that data encryption, staff awareness, and evolving policy controls significantly enhance both data integrity and customer confidence in online financial transactions.

4.8 Network Security Standards and Security of Online Banking Transactions

The study aimed to examine how network security standards influence the security of online banking transactions in Kenya's commercial banks. The results are shown in the table below.

TABLE 4. 6: NETWORK SECURITY STANDARDS

Statement	Mean	Std Dev
1. The network security standards in place effectively protect online banking transactions from cyber threats.	4.148	0.812
2. Our bank's network infrastructure is robust enough to handle potential security breaches.	4.084	0.858
3. Regular updates to network security protocols enhance the safety of online banking transactions.	4.123	0.832
4. Staff training on network security standards is sufficient to mitigate risks associated with online banking.	4.045	0.889
5. The bank's network security measures prevent unauthorized access to sensitive customer information.	4.101	0.841
6. The bank implements industry best practices for network security to ensure the safety of online transactions.	4.076	0.864

Statement	Mean	Std Dev
7. The network security standards contribute to customer confidence in using online banking services.	4.092	0.857
Overall Mean	**4.096**	

The findings of the study showed that a majority of the respondents agreed that the network security standards in place effectively protect online banking transactions from cyber threats, as shown by a mean of 4.148 (Std Dev = 0.812). In addition, the results of the study showed that a majority of the respondents indicated their agreement with the statement that their bank's network infrastructure is robust enough to handle potential security breaches, as shown by a mean of 4.084 (Std Dev = 0.858). The study also found that a majority of the respondents agreed that regular updates to network security protocols enhance the safety of online banking transactions, as shown by a mean of 4.123 (Std Dev = 0.832). Additionally, most respondents agreed that staff training on network security standards is sufficient to mitigate risks associated with online banking, as shown by a mean of 4.045 (Std Dev = 0.889).

A majority of the respondents also agreed that the bank's network security measures prevent unauthorized access to sensitive customer information, as shown by a mean of 4.101 (Std Dev = 0.841). Furthermore, the results showed that a majority of the respondents agreed that the bank implements industry best practices for network security to ensure the safety of online transactions, as shown by a mean of 4.076 (Std Dev = 0.864). Also, a majority of the respondents agreed that the network security standards contribute to customer confidence in using online banking services, as shown by a mean of 4.092 (Std Dev = 0.857). The findings concur with the study conducted by Alshamrani and Singh (2020), which showed that banks implementing comprehensive network security policies, including staff training and real-time security updates are more likely to prevent security breaches and foster customer trust in online banking platforms.

4.9 Institutional Resources

The study sought to assess the influence of institutional resources on the relationship between the implementation of the Central Bank of Kenya's Guideline on Cybersecurity for Payment Service Providers (CBK GCPSP) and the security of online banking transactions in commercial banks. The results are summarized in the table below.

TABLE 4. 7: INSTITUTIONAL RESOURCES

Statement	Mean	Std Dev
1. Financial resources are adequately allocated to implement CBK GCPSP for secure online banking transactions.	4.128	0.824
2. The technological infrastructure in the bank is sufficient to support the secure implementation of CBK GCPSP.	4.095	0.831
3. The bank has enough human capital with the necessary skills to effectively implement the CBK GCPSP.	4.062	0.847
4. The bank regularly invests in upgrading their technological infrastructure to ensure it can meet cyber security requirements.	4.134	0.814
5. Financial resources are prioritized for cyber security initiatives within the bank.	4.101	0.839
6. The bank provides adequate training and development programs for their staff to stay updated on cyber security trends and practices.	4.110	0.822
7. The bank has established a dedicated cyber security team to ensure the implementation of CBK GCPSP.	4.089	0.837
Overall Mean	**4.103**	

The findings of the study showed that a majority of the respondents agreed that financial resources are adequately allocated to implement CBK GCPSP for secure online banking transactions, as shown by a mean of 4.128 (Std Dev = 0.824). In addition, the results of the study showed that a majority of the respondents indicated their agreement with the statement that the technological infrastructure in the bank is sufficient to support the secure implementation of CBK GCPSP, as shown by a mean of 4.095 (Std Dev = 0.831). The study also found that a majority of the respondents agreed that the bank has enough human capital with the necessary skills to effectively implement the CBK GCPSP, as shown by a mean of 4.062 (Std Dev = 0.847). Furthermore, most respondents agreed that the bank regularly invests in upgrading their technological infrastructure to ensure it can meet cyber security requirements, as shown by a mean of 4.134 (Std Dev = 0.814).

A majority of the respondents also agreed that financial resources are prioritized for cyber security initiatives within the bank, as shown by a mean of 4.101 (Std Dev = 0.839). Similarly, a majority of the respondents agreed that the bank provides adequate training and development programs for their staff to stay updated on cyber security trends and practices, as shown by a mean of 4.110 (Std Dev = 0.822). Lastly, the findings indicated that a majority of the respondents agreed that the bank has established a dedicated cyber security team to ensure the implementation of CBK GCPSP, as shown by a mean of 4.089 (Std Dev = 0.837). The findings concur with the study conducted by Karanja and Mureithi (2020), which showed that sufficient financial, technological, and human capital resources significantly enhance the successful implementation of cybersecurity frameworks in the banking sector, improving resilience and trust in digital banking platforms.

Section G: Security of Online Banking Transactions

This research sought to assess the extent to which customers perceive the security of online banking transactions in commercial banks in Kenya. The summarized results are shown in the table below.

TABLE 4. 8: SECURITY OF ONLINE BANKING TRANSACTIONS

Statement	Mean	Std Dev
1. My bank provides secure login features (e.g., two-factor authentication) for online banking.	4.140	0.808
2. I feel confident that my personal and financial information is protected.	4.112	0.817
3. My bank frequently updates its security features to prevent cyber threats.	4.096	0.829
4. I have never experienced unauthorized access or suspicious activity on my online banking account.	4.021	0.846
5. I receive timely alerts from my bank for all transactions carried out online.	4.110	0.831
6. My bank educates customers on safe practices for online banking (e.g., avoiding phishing scams).	4.078	0.823
7. I trust the encryption and data protection mechanisms used by my bank.	4.126	0.816
Overall Mean	**4.098**	

The findings of the study showed that a majority of the respondents agreed that their banks provide secure login features such as two-factor authentication, as shown by a mean of 4.140 (Std Dev = 0.808). In addition, the results of the study showed that a majority of the respondents indicated their agreement with the statement that they feel confident their personal and financial information is protected, as shown by a mean of 4.112 (Std Dev = 0.817). Moreover, most respondents agreed that their bank frequently updates its security features to prevent cyber threats, as shown by a mean of 4.096 (Std Dev = 0.829). A majority of respondents also agreed that they have never experienced unauthorized access or suspicious activity on their online banking accounts, as shown by a mean of 4.021 (Std Dev = 0.846).

The findings further showed that most respondents receive timely alerts from their banks for all online transactions, as shown by a mean of 4.110 (Std Dev = 0.831). A majority also agreed that their banks educate them on safe practices for online banking, such as avoiding phishing scams, as indicated by a mean of 4.078 (Std Dev = 0.823). Lastly, a majority agreed that they trust the encryption and data protection mechanisms used by their banks, as shown by a mean of 4.126 (Std Dev = 0.816). The findings concur with the study conducted by Njoroge and Gitau (2020), which showed that frequent security updates, secure authentication methods, and customer education on cybersecurity significantly improve customer confidence and enhance the perceived security of online banking platforms.

4.10 Inferential Statistics

4.10.1 Multicollinearity Test

A multicollinearity test was carried out by use of Variance Inflation Factors (VIFs) and tolerance levels. A tolerance close to 1 indicates that there is little multicollinearity, whereas a value close to 0 is an indicator for multicollinearity problems (Curto & Pinto, 2007; Schieren & Carr, 1982). The VIF indicates how much the variance of the coefficient estimate is being inflated by multicollinearity. The largest VIF among the independent variables was used to check. The study results were presented in Table 4.11

Table 4.11 Multicollinearity Test

Variables	Tolerance	VIF
Access Control Measures	0.672	1.488
Incident Response	0.701	1.426
Data Protection and Encryption Protocols	0.659	1.517
Network Security Standards	0.683	1.464
Institutional Resources	0.724	1.381

The results in Table 4.11 revealed that tolerance values and variance inflation factor (VIF) values for Access Control Measures were (Tolerance = 0.672, VIF = 1.488). Incident Response was (Tolerance = 0.701, VIF = 1.426), Data Protection and Encryption Protocols were (Tolerance = 0.659, VIF = 1.517), Network Security Standards were (Tolerance = 0.683, VIF = 1.464), and Institutional Resources were (Tolerance = 0.724, VIF = 1.381). Therefore, both the VIFs and tolerance values showed that multicollinearity was not adverse when interpreting the findings of the multivariate analysis. According to Hair, Ring, and Sarstedt (2013), when the VIF is greater than 5 (tolerance < 0.20), then the regression coefficients are poorly estimated. In this study, all the VIF values were below 5 and tolerance values were above 0.20, confirming that multicollinearity was not a problem among the independent variables.

4.10.2 Correlation Analysis

Pearson's Correlation analysis was employed in this study to examine the relationships between various factors influencing the security of online banking transactions. The primary objective was to understand how independent variables such as access control measures, incident response, data protection and encryption protocols, network security standards, and institutional resources correlate with the dependent variable, security of online banking transactions. This analysis helps to identify the strength and direction of these relationships, providing valuable insights into which factors have the most significant impact on the security of online banking platforms.

The correlation coefficients, ranging from -1 to +1, were calculated to assess the degree of association between these variables. A positive correlation indicates that as one variable increases, the other tends to increase as well, whereas a negative correlation would suggest that an increase in one variable corresponds to a decrease in the other. The statistical significance of each

correlation was also tested using p-values to ensure that the observed relationships were not due to random chance. This analysis served as a foundation for understanding how various security measures interact and contribute to the overall protection of online banking transactions, offering crucial information for improving security protocols and addressing potential vulnerabilities.

TABLE 4. 12: PEARSON CORRELATION COEFFICIENTS

Variable	Security of Online Banking Transactions	Access Control Measures	Incident Response	Data Protection and Encryption Protocols	Network Security Standards	Institutional Resources
Security of Online Banking Transactions	1					
Access Control Measures	0.748**	1				
Incident Response	0.679**	0.562**	1			
Data Protection and Encryption Protocols	0.813**	0.708**	0.756**	1		
Network Security Standards	0.790**	0.689**	0.773**	0.838**	1	
Institutional Resources	0.594**	0.503**	0.574**	0.617**	0.590**	1

The results showed a strong positive relationship between security of online banking transactions and access control measures ($r = 0.748$, p-value = 0.000). The p-value of 0.000 is less than the significance level of 0.05, indicating that this relationship is statistically significant. This finding suggests that stronger access control measures, such as multi-factor authentication and robust password policies, significantly enhance the security of online banking transactions. These results are consistent with studies by Chandran *et al.* (2021), which emphasize the importance of access control in preventing unauthorized access and safeguarding digital transactions.

In addition, the results of the study revealed a moderate to strong positive correlation between security of online banking transactions and incident response (r = 0.679, p-value = 0.000). The p-value of 0.000 indicates a significant relationship at the 0.05 level. This suggests that having an effective incident response system that quickly addresses security breaches plays a crucial role in enhancing online banking security. The findings align with previous studies such as Nguyen *et al*. (2020), which highlight that timely and effective incident management can reduce the impact of potential security breaches in online banking systems.

Further, the results showed that there exists a very strong positive correlation between Security of Online Banking Transactions and Data Protection and Encryption Protocols (r = 0.813, p-value = 0.000). The p-value of 0.000, being less than 0.05, indicates a statistically significant relationship. This suggests that sophisticated data protection and encryption protocols are critical in securing online banking transactions. These findings corroborate existing literature, such as Kumar et al. (2019), which emphasizes on the importance of advanced encryption technologies like SSL/TLS in protecting sensitive customer data from cyber threats.

Moreover, the study found a strong positive relationship between security of online banking transactions and network security standards (r = 0.790, p-value = 0.000). The p-value of 0.000 confirms that the relationship is statistically significant. This indicates that robust network security measures, including firewalls and intrusion detection systems, significantly enhance the security of online banking transactions. These results are in line with studies such as Williams & Brown (2020), which emphasize the need for stringent network security protocols in protecting online financial transactions from cyber-attacks.

The results also showed a moderate positive correlation between security of online banking transactions and institutional resources (r = 0.594, p-value = 0.000). The p-value of 0.000 is less than the 0.05 significance level, indicating that the relationship is statistically significant. This suggests that adequate institutional resources, such as investment in advanced technology and skilled personnel, play an important role in enhancing the security of online banking transactions. These findings support previous research by Lamberts (2018), which emphasizes the critical role that organizational resources, including budget allocation and staff expertise, play in implementing effective cybersecurity measures.

4.10.2 Multiple Regression Analysis

In order to assess the influence of the independent variables on the security of online banking transactions, multiple regression analysis was performed. This helped in determining the degree to which each of the independent variables including: Access Control Measures, Incident Response, Data Protection and Encryption Protocols, Network Security Standards, and Institutional Resources, predicted the Security of Online Banking Transactions.

TABLE 4. 13: MODEL SUMMARY

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.875	0.766	0.756	0.286

The R-value of 0.875 indicates a strong positive correlation between the independent variables and the dependent variable (Security of Online Banking Transactions). The R-square value of 0.766 suggests that approximately 76.6% of the variance in online banking security can be explained by the independent variables. This is a strong indication that the model is a good fit for the data. The Adjusted R-square value of 0.756 confirms the robustness of the model, accounting for the number of predictors in the model. Lastly, the standard error of the estimate is 0.286, indicating that the model's predictions are reasonably accurate with small deviations from the observed values.

TABLE 4. 14: ANOVA

Source	Sum of Squares	df	Mean Square	F	Sig.
Regression	103.485	5	20.697	81.053	0.000
Residual	31.739	190	0.180		
Total	135.224	193			

a. Dependent Variable: Security of Online Banking Transactions

b. Predictors: (Constant), Access Control Measures, Incident Response, Data Protection and Encryption Protocols, Network Security Standards, Institutional Resources

The ANOVA results show that the F-value of 81.053 is highly significant ($p < 0.000$), indicating that the overall regression model is statistically significant and that the independent variables together significantly predict the security of online banking transactions. The p-value of 0.000

confirms that the model's predictors have a strong relationship with the dependent variable, suggesting that Access Control Measures, Incident Response, Data Protection and Encryption Protocols, Network Security Standards, and Institutional Resources collectively contribute to the security of online banking systems.

TABLE 4.15: REGRESSION COEFFICIENTS

Variable	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Std. Error		
Constant	0.354	0.095	3.726	0.000
Access Control Measures	0.209	0.045	4.653	0.000
Incident Response	0.176	0.054	3.250	0.001
Data Protection and Encryption Protocols	0.267	0.053	5.038	0.000
Network Security Standards	0.231	0.049	4.725	0.000
Institutional Resources	0.138	0.052	2.654	0.009

Dependent Variable: Security of Online Banking Transactions

The regression equation for the study is as follows:

$$\mathbf{Y = 0.354 + 0.209X_1 + 0.176X_2 + 0.267X_3 + 0.231X_4 + 0.138X_5}$$

From the study, the constant term represents the baseline security of online banking transactions when all independent variables (access control measures, incident response, data protection, network security, and institutional resources) are zero. The value of 0.354 indicates that even in the absence of contributions from these independent variables, the security of online banking transactions remains positive. The p-value of 0.000 confirms the significance of the constant term at the 0.05 level.

The study found that access control measures have a positive and statistically significant effect on the security of online banking transactions ($\beta 1 = 0.209$, $p = 0.000$). This means that for every unit increase in access control measures, such as multi-factor authentication or stronger password policies, the security of online banking transactions is expected to increase by 0.209 units. The p-

value of 0.000 indicates that this relationship is statistically significant at the 0.05 level, reinforcing the importance of access control measures in securing online banking systems.

The study found that incident response capabilities have a positive and statistically significant effect on the security of online banking transactions ($\beta 2 = 0.176$, $p = 0.001$). This means that for every unit increase in incident response measures, such as faster response times to security breaches, the security of online banking transactions is expected to increase by 0.176 units. The p-value of 0.001 indicates that this relationship is statistically significant at the 0.05 level, underlining the critical role of incident response in ensuring the security of online banking platforms.

The study established that data protection and encryption protocols have a positive and statistically significant effect on the security of online banking transactions ($\beta 3 = 0.267$, $p = 0.000$). This means that for every unit increase in data protection and encryption measures, such as stronger encryption algorithms and secure data storage protocols, the security of online banking transactions is expected to increase by 0.267 units. The p-value of 0.000 indicates that this relationship is highly statistically significant, emphasizing the crucial role of encryption and data protection in safeguarding sensitive customer information in online banking.

The study found that network security standards have a positive and statistically significant effect on the security of online banking transactions ($\beta 4 = 0.231$, $p = 0.000$). This means that for every unit increase in network security standards, such as better firewall protections and intrusion detection systems, the security of online banking transactions is expected to increase by 0.231 units. The p-value of 0.000 indicates that this relationship is statistically significant at the 0.05 level, highlighting the importance of robust network security measures in preventing cyberattacks and enhancing online banking security.

The study revealed that institutional resources have a positive and statistically significant effect on the security of online banking transactions ($\beta 5 = 0.138$, $p = 0.009$). This means that for every unit increase in institutional resources, such as increased funding and technology allocation, the security of online banking transactions is expected to increase by 0.138 units. The p-value of 0.009 indicates that this relationship is statistically significant, suggesting that financial institutions must allocate sufficient resources to improve online banking security and meet evolving cybersecurity challenges.

The regression analysis shows that all the independent variables including; access control measures, incident response, data protection and encryption protocols, network security standards, and institutional resources positively influence the security of online banking transactions. These factors are crucial for ensuring a secure online banking environment, and financial institutions should prioritize them to protect customer data and maintain trust in their digital services.

4.11 Chapter Summary

This chapter has presented the nature of research philosophy that was adopted for this study, as well as discussed, the type of research design, population and sampling technique employed in this study, together with the data collection methods used. In addition, the chapter outlined the process that was used to test for reliability and validity and provides the results of these tests. Furthermore, the chapter has presented information on the tests of statistical assumptions that were carried out linearity, homogeneity and multicollinearity.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter provides a comprehensive overview of the summary of findings for the study, drawn conclusions and recommendations. This section aims to summarize the significant results derived from the research, interpret their implications for organizational practices, and offer practical guidance based on the study's findings.

5.2 Summary of Findings

This section provides a discussion of the study's findings, organized according to each research objective.

5.2.1 Access Control and Security of Online Banking Transactions

The findings of the study revealed that employees generally perceive the security controls implemented by their banks as highly effective in safeguarding online banking transactions. Respondents indicated that the existing security measures in their institutions offer strong protection against threats and foster a secure online environment. They expressed confidence in these controls, acknowledging that the systems in place are not only reliable but also play a crucial role in reducing the risk of fraud and unauthorized access to online accounts. In addition, the findings indicated that the access control systems used by banks instill a sense of safety among customers, particularly during online transactions. Respondents appreciated the balance maintained between robust security and user accessibility, noting that the systems are largely user-friendly and do not present unnecessary challenges. The study further revealed that most respondents believe the bank’s security controls are aligned with best practices in protecting sensitive client information, including both personal and financial data. This comprehensive protection contributes significantly to customer confidence and trust in digital banking platforms.

However, while the general perception was positive, the aspect of user-friendliness in some security measures emerged as an area with relatively lower levels of agreement. This suggests that while customers value stringent security, there is a need to ensure these controls remain accessible and convenient to use. Improving the usability of security features may further enhance user

satisfaction and encourage more frequent engagement with online banking services. From the researcher's perspective, these findings underscore the importance of investing in robust and practical security measures that not only safeguard digital transactions but also foster customer trust. The positive perceptions reflect that customers value protection mechanisms that are both comprehensive and easy to use. However, the slight reservations around usability signal the need for continuous improvement in digital security design—particularly the need for systems that are intuitive and accessible to a wide range of users. Banks should adopt a client-centric approach in enhancing their digital platforms, ensuring that security does not come at the cost of convenience. Creating such a balance is critical in advancing digital trust, customer satisfaction, and sustained use of online banking services.

These findings concur with the study by Al-Emran, Shaalan, and Al-Kabi (2020), which demonstrated that trust in online banking is significantly influenced by strong access control systems, user-friendly security features, and the overall perception of data safety. Their study emphasized that effective digital security practices enhance user confidence and encourage the adoption of banking technologies. Similarly, a study by Mutua and Mwania (2021) in the Kenyan banking sector found that reliable cybersecurity infrastructure and regular updates to security protocols were directly linked to increased customer loyalty and online banking adoption. Their research highlighted that customers are more likely to trust and utilize digital platforms that prioritize safety. In addition, research by Osei and Boateng (2022) revealed that transparency in security measures, multi-factor authentication, and proactive fraud detection systems significantly improved customer confidence and reduced the incidence of online fraud in West African banks. These findings affirm the critical role of visible and functional security mechanisms in shaping positive customer experiences.

5.2.2 Incidence Response and Security of Online Banking Transactions

The findings of the study revealed that employees generally perceive the incident response strategies implemented by their banks as effective in securing online banking operations. Respondents expressed agreement that their institutions have a well-structured and clearly defined incident response plan in place, which is crucial in mitigating security breaches. The study further showed that most employees acknowledged the regular testing and updating of these procedures, demonstrating preparedness for emerging cyber threats. Moreover, the findings indicated that

respondents believe that security incidents are effectively managed and mitigated, with prompt communication provided to customers in the event of any breach. These proactive measures were associated with a greater sense of confidence among employees regarding the overall security of online banking transactions. The study also revealed that banks routinely test their platforms for vulnerabilities and conduct post-incident reviews, which further strengthens their ability to respond to future threats effectively.

Nevertheless, even though the general perception was positive, the area of vulnerability testing and post-incident review showed slightly lower levels of agreement. This highlights an opportunity for institutions to enhance transparency and consistency in how these practices are communicated and implemented. Ensuring all stakeholders are aware of these processes can further reinforce trust in the institution's cybersecurity framework. From the researcher's point of view, these findings emphasize the essential role of structured and proactive incident response mechanisms in maintaining secure digital financial ecosystems. A well-articulated and regularly updated response plan fosters confidence not only among employees but also among customers who rely on online platforms for financial transactions. It is crucial that organizations not only implement these frameworks but also invest in continuous training, real-time threat monitoring, and communication protocols to mitigate the impacts of cyber incidents. Enhancing visibility and feedback mechanisms around incident response can improve preparedness and build long-term trust in online banking services.

These findings concur with the study by Akhter and Sultana (2020), which showed that robust incident response planning, real-time monitoring, and continuous post-event reviews significantly enhance customer trust and reduce the likelihood of recurring cyber incidents in digital banking. Similarly, research by Barasa and Gichuki (2021) in Kenya revealed that banks with formalized incident response frameworks reported fewer instances of prolonged service disruption and improved recovery time following breaches. Their study highlighted the importance of real-time detection tools and rapid communication with affected customers. In addition, a study conducted by Iqbal, Rehman, and Mahmood (2022) emphasized that effective post-incident evaluation and system reinforcement were key components in improving organizational resilience in the face of growing cyber threats. Their findings align with the current study in affirming that comprehensive incident response contributes to the security and continuity of digital financial services.

5.2.3 Data Protection Protocols and Security of Online Banking Transactions

The findings of the study revealed that a majority of respondents agreed that data protection and encryption mechanisms implemented by their banks are effective in safeguarding customer information. Respondents affirmed that their banks have strong data protection policies that shield sensitive information from unauthorized access. The study also highlighted that the encryption protocols in place are perceived as adequate in securing customer data against cyber threats, with systems believed to be capable of preventing data breaches and ensuring data confidentiality. Further, the respondents acknowledged that staff are sufficiently trained to handle sensitive data responsibly, which is critical in ensuring the security of personal and financial information. The findings also showed that banks regularly update their data protection and encryption protocols to respond to the rapidly evolving threat landscape. Additionally, respondents agreed that their banks take active steps to comply with data protection regulations, which enhances institutional credibility and accountability.

Moreover, respondents indicated that data protection and encryption mechanisms significantly contribute to customer trust. When banks demonstrate a strong commitment to securing sensitive information, customers are more confident in using online banking platforms, reinforcing loyalty and usage frequency. Overall, the findings suggest that there is a high level of agreement among employees that data protection and encryption are key components of a secure digital banking environment.

From the researcher's perspective, these findings reinforce the critical importance of data protection and encryption in the digital financial space. Strong encryption protocols and clearly defined data protection policies form the foundation of trust between banking institutions and their customers. Moreover, the combination of technological safeguards and continuous staff training builds institutional resilience against internal and external threats. As threats become increasingly sophisticated, banks must not only rely on technical solutions but also promote a culture of data responsibility and compliance. Sustained investment in security infrastructure and capacity building is essential in preserving customer confidence and ensuring business continuity in the face of cyber risks.

These findings concur with the study conducted by Furnell and Shah (2020), which demonstrated that effective data encryption, coupled with staff awareness and evolving policy frameworks, significantly enhances the integrity of data and fosters greater trust in online financial platforms. Similar conclusions were drawn in a study by Wanjiru and Kihoro (2021) in Kenya, which found that institutions that prioritize data privacy, staff training, and compliance with data protection laws recorded higher levels of customer satisfaction and reduced cyber incidents. Additionally, the research by Zhao, Li, and Song (2022) emphasized that regular updates to encryption protocols, regulatory compliance, and multi-layered protection frameworks were instrumental in minimizing vulnerabilities and building trust in online banking systems across digital platforms in Asia.

5.2.4 Network Security Standards and Security of Online Banking Transactions

On this objective, the findings of the study revealed that a majority of the respondents agreed that the network security standards adopted by their banks are effective in protecting online banking transactions from potential cyber threats. Respondents expressed confidence in the robustness of their bank's network infrastructure, stating that it is well-equipped to handle potential breaches and ensure the continuity of secure services. They further affirmed that regular updates to network security protocols play a vital role in enhancing the overall safety of digital banking activities. In addition, the study found that employees perceive staff training on network security as adequate, contributing to the institution's preparedness in managing threats related to unauthorized access and cyberattacks. Respondents also agreed that network security measures in their banks are aligned with industry best practices, which include layered security approaches, proactive threat detection systems, and secure firewalls. These practices were seen as key in preventing the compromise of sensitive customer data.

Moreover, the findings highlighted that network security standards contribute to customer confidence in using online banking services. When customers are assured of the institution's capability to secure digital channels, their trust in and reliance on online banking systems is strengthened. Overall, the results suggest that network security is not only a technical function but also a critical trust-building mechanism in the digital financial ecosystem. From the researcher's perspective, these findings underscore the fundamental role that network security plays in modern banking operations. Strong and adaptive network security standards act as the first line of defense

against ever-evolving cyber threats. It is evident that the combination of reliable infrastructure, continuous staff training, and adherence to global best practices significantly enhances an institution's ability to offer secure digital services. As the threat landscape grows more complex, the emphasis must not only be on reactive measures but also on a proactive culture of cybersecurity awareness and strategic investments in secure network design.

These findings concur with the study conducted by Alshamrani and Singh (2020), which found that banks that implement comprehensive network security frameworks, regular protocol updates, and continuous staff training are better positioned to avoid cyber incidents and increase customer trust in online banking platforms. Similar conclusions were reported by Mugo and Waweru (2021) in a Kenyan context, where it was established that robust network defenses, periodic assessments, and alignment with industry standards contributed to enhanced consumer protection and reduced vulnerability to external attacks. Additionally, the study by Rana, Jena, and Pradhan (2022) supported the importance of adopting dynamic network security policies and active risk management systems, emphasizing their impact on customer satisfaction, institutional resilience, and long-term trust in digital financial environments.

5.2.5 Institutional Resources, CBK Cybersecurity Guidelines CBK and Security of Online Banking Transactions

The findings of the study showed that a majority of the respondents agreed that financial resources are adequately allocated to implement the CBK GCPSP for secure online banking transactions. Similarly, the results revealed that most respondents agreed that the technological infrastructure in the bank is sufficient to support the secure implementation of CBK GCPSP. The study also found that the majority of respondents agreed that the bank has enough human capital with the necessary skills to effectively implement the CBK GCPSP.

Furthermore, most respondents agreed that the bank regularly invests in upgrading its technological infrastructure to ensure it meets cybersecurity requirements. Respondents also indicated that financial resources are prioritized for cybersecurity initiatives within the bank. Similarly, most respondents agreed that the bank provides adequate training and development programs for staff to stay updated on cybersecurity trends and practices. Lastly, the findings

indicated that the majority of respondents agreed that the bank has established a dedicated cybersecurity team to ensure the successful implementation of CBK GCPSP.

According to the views of the researcher, these findings highlight the significant investment made by banks in financial, technological, and human capital resources to support the effective implementation of the CBK GCPSP. The study underscores the importance of allocating adequate resources for secure online banking transactions, particularly in terms of infrastructure, human expertise, and continuous training. It is clear that such investments not only enhance cybersecurity but also contribute to building trust in digital banking services. The proactive measures taken by banks, including regular infrastructure upgrades and the establishment of dedicated cybersecurity teams, reflect a strong commitment to safeguarding digital platforms and maintaining consumer confidence.

These findings concurred with the study by Karanja and Mureithi (2020), which demonstrated that the successful implementation of cybersecurity frameworks in the banking sector requires sufficient financial, technological, and human resources. This alignment is crucial in enhancing resilience and fostering trust in online banking platforms. Similar conclusions were drawn by Kim, Park, and Lee (2021), who found that a well-structured investment in cybersecurity infrastructure and employee training enhances banks' ability to prevent cyber threats and increases customer satisfaction. Additionally, the study by Ochieng and Ngugi (2022) supports these findings, noting that regular investments in cybersecurity measures and the recruitment of skilled personnel significantly improve banks' ability to manage and mitigate risks in online banking environments.

5.3 Conclusions of the Study

5.3.1 Access Control and Security of Online Banking Transactions

On this objective, the study concluded that security controls play a significant role in enhancing the security of online banking transactions. This conclusion is based on employees' perceptions that the existing security systems in their banks are effective, reliable, and instrumental in protecting against fraud and unauthorized access. The findings suggest that access control measures are not only robust but also generally user-friendly, which contributes to a safe and seamless digital banking experience. Moreover, the alignment of these security controls with

industry best practices reinforces customer confidence by ensuring the protection of sensitive personal and financial information. However, the study also notes that the aspect of user-friendliness in some security features received relatively lower levels of agreement, indicating a need to improve the accessibility and ease of use of these systems. These findings collectively affirm that secure, intuitive, and well-designed digital security frameworks are essential in fostering customer trust and promoting sustained engagement with online banking services.

5.3.2 Incidence Response and Security of Online Banking Transactions

The study concluded that incident response mechanisms are pivotal in enhancing security of online banking transactions. This conclusion is grounded in employees' perceptions that their banks have well-defined and actively managed incident response plans capable of mitigating cyber threats. The findings indicate that most institutions consistently test and update their response strategies, which fosters organizational readiness and resilience. Additionally, prompt communication with customers in the event of security breaches has been recognized as a contributing factor in reinforcing public trust. The study highlights that while the general sentiment toward incident response systems is positive, slightly lower agreement levels on vulnerability testing and post-incident reviews suggest a need to strengthen transparency and consistency in these areas. Therefore, the findings affirm that structured, proactive, and well-communicated incident response frameworks are essential in building confidence in digital banking environments and in ensuring effective handling of cyber threats.

5.3.3 Data Protection Protocols and Security of Online Banking Transactions

The study concluded that data protection and encryption protocols significantly contribute to the security of online banking transactions. Employees widely agreed that their banks' systems are effective in preventing unauthorized access and safeguarding sensitive customer information. The findings reveal that not only are the encryption mechanisms considered reliable, but banks also provide adequate staff training on secure data handling, which reinforces a culture of responsibility and trust. Furthermore, the study found that adherence to regulatory standards and the regular updating of security measures improve customer confidence and institutional accountability. These results affirm that data protection efforts when integrated with comprehensive training, strong policies, and technical safeguards form the bedrock of secure digital banking systems. As

the cyber threat landscape continues to evolve, continuous improvement in these areas remains vital for customer trust and sustained use of online financial services.

5.3.4 Network Security Standards and Security of Online Banking Transactions

The study concluded that strong network security standards play a critical role in security of online banking transactions. Employees perceived their banks' network infrastructures as well-fortified, frequently updated, and aligned with global cybersecurity practices. The findings suggest that layered security measures, proactive threat detection, and reliable firewalls form an effective defense against cyber-attacks. Additionally, staff training in network security was found to be adequate, contributing to organizational preparedness. The study emphasized that these network safeguards not only prevent security breaches but also foster customer confidence by assuring them of the reliability and resilience of online banking systems. Nevertheless, continuous investment in adaptive and anticipatory security approaches is essential as cyber risks become increasingly complex. The findings support the view that robust network defenses are integral not only to technical resilience but also to the overall perception of safety in digital financial ecosystems.

5.3.5 Institutional Resources, CBK Cybersecurity Guidelines CBK and Security of Online Banking Transactions

The study concluded that the allocation of institutional resources including financial, technological, and human are all fundamental to the successful implementation of the CBK GCPSP and the overall security of online banking systems. Employees acknowledged that their banks invest significantly in upgrading infrastructure, training personnel, and establishing dedicated cybersecurity teams to ensure alignment with the CBK cybersecurity guidelines. The findings highlight that banks' commitment to regular updates, compliance efforts, and staff development fosters a secure and resilient online environment. This strategic resource allocation also reflects a broader institutional culture that prioritizes digital safety and regulatory adherence. However, ongoing investment and strategic planning are needed to adapt to the dynamic threat landscape. These findings confirm that resource mobilization and capacity building are not only enablers of compliance but also key drivers of trust and operational excellence in digital banking platforms.

5.4 Recommendations of the Study

This study recommends that banks prioritize strengthening and regularly updating their incident response plans, including conducting simulated exercises to enhance preparedness for cyber threats. It is essential to ensure transparency in vulnerability testing and post-incident reviews, with clear communication protocols for all stakeholders involved. Additionally, banks should invest in real-time threat detection systems and maintain open communication with customers during security incidents, fostering confidence in the institution's ability to respond effectively. Ongoing training for employees on handling cyber incidents is also critical to maintaining a well-prepared workforce.

In addition, this study recommends that banks implement and continuously update encryption and data protection systems in line with the latest industry standards. Regular training should be provided to employees to ensure that they understand and uphold data protection policies. Moreover, banks should adopt multi-layered data protection strategies, such as tokenization and anonymization, to further safeguard customer data. Ensuring compliance with data protection regulations through audits and monitoring is necessary, alongside fostering a culture of data privacy across the organization.

Also, the study recommends that banks update network security protocols regularly and implement frequent system patches to prevent vulnerabilities. Continuous training for IT staff on emerging cybersecurity threats is essential to keeping up with evolving risks. Banks should also invest in advanced network security tools such as intrusion detection systems and endpoint protection, conduct regular penetration testing, and perform network risk assessments to identify and mitigate potential threats. Collaborating with cybersecurity experts and regulatory bodies will ensure that banks stay aligned with best practices and emerging challenges in the cybersecurity landscape.

Finally, this study recommends that banks should allocate sufficient financial resources to effectively implement the Central Bank of Kenya's (CBK) Cybersecurity Guidelines for Secure Online Banking Transactions (GCPSP). Regular upgrades to technological infrastructure are crucial to ensure compliance with cybersecurity standards, and sufficient investment in hiring and retaining skilled cybersecurity professionals will bolster the institution's defense mechanisms. Establishing dedicated cybersecurity teams and prioritizing employee training in best practices are

vital to ensuring the successful implementation of CBK's guidelines and maintaining customer trust.

5.5 Recommendations for Further Studies

This study recommends that future research should explore the long-term impact of evolving cybersecurity frameworks on customer trust and satisfaction in online banking. Additionally, further studies could examine the effectiveness of emerging technologies, such as artificial intelligence and machine learning, in detecting and preventing cyber threats within digital banking systems. It would also be valuable to investigate the role of customer awareness and education on cybersecurity measures, as well as the influence of regulatory changes on banking institutions' security practices. Further studies could also conduct comparative research between different countries or regions could provide insights into the global trends and challenges in securing online banking transactions.

5.6 Research Contributions

The study has identified major threats such as phishing, social engineering, and malware as significant risks to digital banking platforms. Effective implementation of CBK guidelines has been linked to improved risk management, stronger regulatory compliance, and enhanced ICT infrastructure. Employee training and customer awareness have emerged as critical factors in mitigating cyber threats, while technological measures like multi-factor authentication and biometric security have significantly improved system resilience. Additionally, research emphasizes the need for board-level accountability, comprehensive vendor risk management, and the adoption of robust cyber risk frameworks to address vulnerabilities, especially those introduced by third-party service providers and fintech integrations. Overall, these findings support a holistic approach to cybersecurity, aligning strategic, technical, and regulatory efforts to safeguard online banking operations.

5.7 Limitations of the study.

The data collection process was limited by strict timelines, which affected the depth of engagement with some respondents. As a result, some responses may have lacked the detail or reflection that could have been achieved with more time. In order to overcome the limitation, the study was designed to be conducted within a specific academic schedule and timeframe, necessitating a concise data collection period.

References

Adeyemi, A. (2021). Cybersecurity standards and frameworks in Africa: A case study of South Africa and Nigeria. *African Journal of Information Security*, 12(1), 22-37.

Agwu, M. E. (2022). Information security and online banking in developing economies: A Nigerian perspective. *International Journal of Information Technology and Computer Science*, 10(3), 33-45.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Akhter, S., & Sultana, R. (2020). The role of incident response management in enhancing online banking security in developing economies. *International Journal of Information Security and Privacy, 14*(3), 45–61.

Akinmoladun, F. A., & Adeyemi, A. S. (2020). Institutional resources and cybersecurity in Nigerian commercial banks: The role of technology and skilled personnel. *International Journal of Cybersecurity and Digital Forensics, 8*(2), 44-58.

Al-Emran, M., Mezhuyev, V., & Kamaludin, A. (2020). Technology adoption in higher education: A systematic review of diffusion of innovation theory. *International Journal of Emerging Technologies in Learning, 15*(20), 45-60.

Alshamrani, A., & Singh, M. (2020). *A comprehensive review on the security of online banking systems*. Journal of Cybersecurity and Information Management, 8(2), 45–60.

Amankwah-Amoah, J. (2020). Cyber security challenges in Africa: Insights from Nigeria and South Africa. *African Journal of Information Systems*, 8(4), 58-69.

Anderson, J. (2020). Multi-layered data protection in banking: Best practices for secure online transactions. *Journal of Cybersecurity and Privacy*, 18(3), 201-214.

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. F. (2017). *Sampling and sampling methods*. *Research Journal of Educational Studies and Reviews*, 3(4), 1-11.

Bagozzi, R. P. (2007). The legacy of the Technology Acceptance Model and a proposal for a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 244-254.

Bansal, P. (2022). Global trends in cybersecurity regulation: An analysis of the European Union's GDPR and PSD2. *Journal of Global Financial Regulations*, 23(2), 15-27.

Brar, S. (2022). Cybersecurity threats in the banking sector: Addressing the evolving risks. *Journal of Financial Security and Risk Management*, 19(3), 56-69.

Bryman, A. (2016). *Social research methods* (5th Ed.). Oxford University Press. Bryman, A., & Bell, E. (2015). *Business research methods* (4th Ed.). Oxford University Press.

CBK. (2019). *Guideline on Cybersecurity for payment service providers July 2019.* Central Bank of Kenya.

CBK. (2024). Cybersecurity in Financial Institutions: Policy and Best Practices. Nairobi: Central Bank of Kenya.

Central Bank of Kenya (CBK). (2019). *Guideline on Cybersecurity for payment service providers July 2019:* Central Bank of Kenya.

Central Bank of Kenya. (2020). *ICT Risk Management Guidelines* (Version 2.0). Central Bank of Kenya.

Central Bank of Kenya. Bank Supervision Dept. (2023). *Bank supervision annual report*. Central Bank of Kenya.

Central Bank of Kenya. (2024). *Financial sector stability report 2024*.

Charness, N., & Boot, W. R. (2020). Technology adoption in older adults: Perceptions and recommendations for successful technology use. *Current Directions in Psychological Science, 29*(3), 279-285.

Chavez, R. (2020). *Cybersecurity and access control in online banking: Best practices and trends*. Journal of Financial Security, 15(2), 134-148.

Chen, L., Zhang, Y., & Liu, T. (2020). The role of firewalls and intrusion detection systems in secure online banking. *Journal of Financial Security*, 23(3), 56-70.

Chung, T. (2020). Data protection protocols in online banking: Strategies and challenges. *Journal of Cybersecurity in Finance*, 22(1), 34-48.

Communications Authority of Kenya. (2023). *Cybersecurity Report Q4 2022-2023.*

Cooper, D. R. (2020). *Business research methods* (12th Ed.). McGraw-Hill Education.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th Ed.). SAGE Publications.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Dlamini, S. (2023). Enhancing cybersecurity in Africa's banking sector: Challenges and opportunities. *Journal of African Economic Studies*, 30(1), 45-58.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review, 14*(1), 57-74.

European Union Agency for Cybersecurity (ENISA). (2020). *Cybersecurity for digital services in financial sectors: An EU report*. ENISA Publications.

Fama, E. F. (1980). Agency problems and the theory of the firm. *Journal of Political Economy, 88*(2), 288-307.

Furnell, S., & Shah, J. N. (2020). Securing digital financial services: The impact of encryption and data protection practices on user trust. *Journal of Cybersecurity Technology*, *4*(2), 129–147.

Gichuki, R. (2022). The Impact of Rapid Cyber Threats on the Banking Sector in Kenya. *Journal of Cybersecurity and Financial Services*, 6(1), 29-40.

Gikandi, J. W., & Bloor, C. (2020). Digital banking security in Kenya: Examining the role of regulation in mitigating cyber risks. *African Journal of Information Security*, 6(2), 45-60.

Greenhalgh, T., Papoutsi, C., & Shaw, S. (2020). Diffusion of innovations in service organizations: Systematic review and recommendations. *Milbank Quarterly, 98*(3), 411-465.

Harris, L., & Ford, G. (2021). The impact of multi-layer network security systems in banking. *Journal of Cybersecurity & Financial Technology*, 18(2), 134-148.

HF Group Overview. (2025). Available at: https://www.hfgroup.co.ke/about-us Accessed 5 May 2025

Huth, R. (2020). The role of regulatory frameworks in cybersecurity: A comparison of the European Union and the United States. *Journal of International Cyber Law*, 11(1), 67-81.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs, and ownership structure. *Journal of Financial Economics, 3*(4), 305-360.

Jones, A. (2023). Risk management in the banking sector: Cybersecurity guidelines by the Federal Financial Institutions Examination Council (FFIEC). *Journal of American Banking Regulations*, 14(2), 24-35.

Juma, R. (2021). Cybersecurity risks and the banking sector: Managing cyber threats through incident response. *Kenya Banking Review*, 10(1), 45-60.

Kagiri, S., & Gichuki, M. (2021). *The effectiveness of access control measures in securing mobile banking transactions in Kenya*. Journal of Information Security, 22(3), 215-227.

Kamau, N., & Wambua, P. (2020). Enhancing customer awareness of banking security protocols. *Kenya Journal of Cybersecurity Studies*, 18(3), 124-136. University of Nairobi Press.

Kamau, R., & Limo, J. (2021). *The effectiveness of cybersecurity policies in enhancing secure online banking transactions in Kenya*. Journal of Banking and Financial Security, 15(2), 78-92.

Karanja, J., & Mwai, D. (2020). Evaluating the role of financial institutions in addressing cybersecurity challenges in Kenya. *Journal of Cybersecurity and Financial Technology, 12*(2), 34-45.

Karanja, P., & Mureithi, S. (2020). *Institutional capabilities and cybersecurity implementation in commercial banks in Kenya*. African Journal of Information Security and Risk Management, 5(1), 20–35.

Kariuki, D. (2020). Identity theft and phishing attacks: A growing concern in Kenya's online banking sector. *Journal of Financial Cybersecurity*, 8(2), 51-62.

Kariuki, F. (2015). *Sustainability in the financial sector in Kenya* (No. 11). KBA Centre for Research on Financial Markets and Policy Working Paper Series.

Kaur, P. (2020). The impact of cybersecurity challenges on online banking services. *International Journal of Information Security*, 18(2), 112-128.

Kenya Bankers Association. (2020). *Annual Banking Survey*. Kenya Bankers Association.

Khan, F. (2021). Enhancing trust in online banking: The role of cybersecurity regulations. *Global Finance and Security Journal*, 24(1), 35-49.

Kibet, L., & Makau, P. (2020). Enhancing cyber resilience in Kenya's banking sector. *Cybersecurity and Financial Stability Journal*, 5(2), 33-49

Kinyua, E., & Wambua, M. (2020). Artificial intelligence in financial security: Incident response in online banking. *Journal of Cybersecurity*, 19(2), 233-245.

Kirui, C., & Gikaru, D. (2020). Barriers to effective implementation of cybersecurity guidelines in Kenyan commercial banks. *Journal of Banking Security, 11*(5), 45-59.

Kothari, C. R. (2009). *Research methodology: Methods and techniques* (2nd Ed.). New Age International.

Lee, M., & Cho, J. (2020). Implementing security protocols in banking networks to reduce cyber risk. *International Journal of Cybersecurity*, 11(1), 45-59.

Leitner, M. (2020). Cybersecurity and fraud prevention in digital banking: A global perspective. *Journal of Financial Services Regulation*, 21(2), 14-25.

Lien, G. (2020). Corporate governance and agency problems in financial institutions: The role of the board of directors. *Journal of Banking and Finance, 45*(2), 134-152.

Lwamba, R. (2020). Cybersecurity threats in Kenyan banking: Trends and strategies for mitigation. *Cybersecurity and Risk Management Journal*, 5(3), 84-97.

Mackenzie, N., & Knipe, S. (2006). *Research dilemmas: Paradigms, methods, and methodology*. *Issues in Educational Research*, 16(2), 1-15.

Makau, P., & Wambua, L. (2020). The impact of financial illiteracy on digital banking adoption in Kenya. *East African Journal of Economics and Business*, 10(3), 45-58.

Mburu, J. (2020). Risks and challenges in the banking sector: A case study of Kenyan banks. *African Journal of Banking and Finance*, 22(4), 123-136.

Miller, D. (2020). *The role of access control in securing online banking systems*. Cybersecurity

Mugambi, A., & Karanja, T. (2021). Resource constraints and cybersecurity preparedness in the banking sector. *Journal of Financial and Cybersecurity Research*, 19(1), 112-126.

Mugo, E., & Njoroge, K. (2021). Effective incident response frameworks for secure online banking transactions. *International Journal of Banking and Finance*, 29(5), 77-91.

Mukami, K. (2021). Enhancing cybersecurity in financial institutions: A case study of Kenyan banks. *African Journal of Information Technology*, 11(1), 112-126.

Muriuki, R. (2020). An analysis of cybersecurity challenges in Kenya's banking sector. *East African Journal of Cybersecurity*, 4(1), 28-42.

Muthoni, G. (2021). Challenges in the Implementation of Cybersecurity Measures in Kenya's Financial Sector: A Case Study of Smaller Banks. *Kenya Journal of Banking and Finance*, 15(2), 112-130.

Mutiso, L., & Kipkemboi, B. (2021). Cybersecurity risks and financial implications in Kenya's digital banking landscape. *Cybersecurity and Digital Economy, 9*(1), 23-37.

Mutua, A., & Njoroge, J. (2020). *Regulatory measures and their impact on banking security in Kenya: A review of CBK guidelines*. Journal of Financial Regulation, 17(3), 78-92.

Mutuku, J. (2020). Cybersecurity challenges in the Kenyan banking sector: The role of regulatory frameworks. *Journal of African Financial Regulation*, 5(2), 45-57.

Mwangi, R., & Kimani, P. (2021). The effectiveness of Central Bank of Kenya guidelines in reducing cybersecurity threats in financial institutions. *Journal of Financial Regulation and Cybersecurity, 6*(3), 89-102.

Mwangi, R., Kamau, P., & Njoroge, M. (2021). Network security adoption in Kenyan banks: Challenges and progress. *Kenya Financial Security Journal*, 14(3), 78-92.

Mwangi, T. (2020). Cybersecurity risks and the banking sector in Kenya. *East African Cybersecurity Journal*, 6(2), 21-36.

Nderitu, D. (2021). Regulatory challenges and compliance in Kenyan banks: A focus on ICT risk management. *African Banking Review*, 10(1), 65-79.

Ngugi, M. (2021). Securing customer data in online banking systems. *Kenya Journal of Financial Technology*, 11(4), 75-88.

Njeru, C. (2020). Overseeing cybersecurity in Kenyan banks: The role of the Central Bank of Kenya. *Kenya Journal of Banking and Finance*, 13(1), 23-37.

Njogu, F. (2023). A critical review of the implementation of ICT Risk Management Guidelines in Kenya's banking sector. *Kenyan Journal of Financial Security*, 18(1), 35-50.

Njoroge, M. (2021). Strengthening data protection practices in Kenyan commercial banks. *Journal of Financial Security*, 22(1), 99-112.

Njoroge, M., & Gitau, R. (2020). *Determinants of customer trust in online banking security systems in Kenyan commercial banks*. Journal of Financial Services Technology, 6(2), 45–59.

Njoroge, M., & Mwangi, S. (2020). The role of encryption in securing online banking in Kenya. *Journal of Digital Security*, 7(2), 78-91.

Ntim, C. G. (2021). Financial regulations and cybersecurity: A review of global perspectives. *International Journal of Financial Management*, 31(1), 67-80.

O'Neill, B. (2021). Cybersecurity and network protection in financial services: A review. *Journal of Banking Technology*, 29(2), 112-124.

Ochieng, J., & Karanja, M. (2020). Advancing secure online banking in Kenya: The role of technology and regulation. *African Journal of Technology and Security*, 3(2), 67-81.

Ochieng, P., & Mugo, M. (2021). Cyber threats and the role of ICT in Kenya's banking sector. *Journal of African Financial Technology*, 3(4), 42-58.

Odhiambo, P. (2021). The role of commercial banks in financial inclusion in Kenya. *Kenya Journal of Banking and Finance*, 15(2), 34-47.

Ojo, O. (2020). Incident response management in cybersecurity: Strategies for financial institutions. *Journal of Financial Security*, 18(3), 214-228.

Okifo, D. (2021). Online Banking in Kenya: The Road to Financial Inclusion. *Journal of Financial Technology*, 7(3), 210-225.

Okonkwo, A. (2019). Addressing cybersecurity challenges in global banking: An African perspective. *Journal of African Information Security*, 9(2), 34-45.

Okoth, G. (2020). Compliance monitoring in Kenyan financial institutions: The role of the Central Bank of Kenya in ICT risk management. *International Journal of Financial Regulation*, 15(3), 100-115.

Olalekan, O., & Temitope, A. (2021). Mobile banking adoption in Nigeria: Application of Diffusion of Innovations Theory. *Journal of Financial Innovation and Inclusion, 9*(2), 89-104.

Omondi, S. (2020). Small banks and cybersecurity challenges in Kenya: The implications of CBK guidelines. *International Journal of Cybersecurity*, 8(4), 118-132.

Otieno, M., & Kamau, F. (2022). Investigating the relationship between cybersecurity guidelines and financial loss prevention in Kenyan banks. *Journal of Financial Security, 14*(3), 56-70.

Owusu, A., & Boh, W. F. (2021). Adoption of mobile banking services in sub-Saharan Africa: A Technology Acceptance Model perspective. *African Journal of Information Systems, 13*(2), 27-45.

Patel, S., & Singh, R. (2021). *Security measures for financial transactions: An analysis of access control practices in global banking*. Journal of Information and Security, 24(3), 131-145.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Sambasivan, M., & Tan, K. (2020). Network security standards and banking: Enhancing online transaction security. *Journal of Cybersecurity in Finance*, 21(4), 72-85.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th Ed.). Pearson Education.

Schmidt, A., Müller, T., & Weber, S. (2021). Enhancing online banking security through data encryption and tokenization. *European Financial Security Review*, 32(5), 120-134.

Tan, W., Tan, B., & Chen, S. (2020). Enhancing banking security through data protection measures in Southeast Asia. *Asian Journal of Financial Security*, 13(2), 156-171.

Tessema, F., Mutua, L., & Karanja, S. (2020). Automation and real-time monitoring in incident response systems for banks. *European Journal of Cybersecurity*, 22(3), 200-210.

Velasco, C. (2024). Commercial Banking in Kenya: A History from Colonisation to Digital Age. Taylor & Francis.

Wairimu, R. (2022). Compliance Monitoring and Reporting in Kenyan Financial Institutions: The Role of the Central Bank of Kenya. *Journal of Financial Regulation*, 9(4), 77-92.

Wakoli, L. W. (2024). Factors that influence cybersecurity compliance behaviours by bank employees: A case of banks operating in Kenya. *International Journal of Scientific Research and Management (IJSRM)*, *12*(12).

Wambua, P. (2021). The role of incident response in mitigating online banking risks in Kenya. *Kenya Financial Security Journal*, 12(4), 58-72.

Wambui, K., & Mwaura, J. (2021). The impact of cybersecurity risk management strategies on operational efficiency in Kenyan banks. *International Journal of Banking and Financial Services, 18*(4), 102-117.

Wambui, M., & Kiptui, M. (2021). The impact of mobile banking on financial inclusion in rural Kenya. *International Journal of Financial Services*, 18(1), 14-29.

Wamuyu, P. (2020). The challenges of cybersecurity regulation in Kenya's banking sector. *East African Financial Review*, 9(2), 123-138.

Wanjiru, D. (2020). The role of Central Bank of Kenya in regulating online banking security. *Kenya Financial Review, 12*(4), 50-62.

Wanjiru, M. (2020). Cybersecurity standards and financial institutions in Kenya: A look at the CBK's ICT guidelines. *Kenyan Journal of Digital Banking*, 12(2), 77-90.

Wanyama, S. (2020). ICT risk management and its role in securing banking systems in Kenya. *Journal of Information Technology and Banking*, 22(1), 45-58.

APPENDICES

Appendix I: Consent Form

Title of Study: Evaluating the implementation of CBK Cybersecurity Guidelines and their Effect on Online Banking Security: Institutional Resources as a Mediating factor.

Researcher's Details:

Purpose of the Study: The purpose of this study is to assess the effectiveness of CBK GCPSP and the degree of their Implementation on online Banking Transactions in Kenya

Study Procedure: If you consent to take part in this study, you are be requested to complete a questionnaire. The questionnaire takes approximately 20 minutes to complete and your responses will remain confidential, solely for academic research purposes, providing insights into the effectiveness of these GCPSP in securing online banking transactions.

Confidentiality: The information you provide will be exclusively used for data analysis related to the objectives of this study. The results will be employed solely for academic research purposes and to contribute to the body of knowledge in the field of Forensic audit. All personal data and identity-related information will be kept confidential and will not be included in any study reports or publications.

Consent Statement: Any information you provide will be used merely for analysis connected to the objectives of this study. The results will be used wholly for academic research purposes, enhancing the understanding of CBK GCPSP implementation. Any personal data will be kept in total confidentiality and will not be shared in any reports or publications resulting from the study.

I am participating in this study voluntarily. I am fully aware that the responses I provide remain confidential.

Date: _____

For any further consultations, feel free to contact the researcher, using the details provided at the beginning of this consent letter.

Thank you for your cooperation.

Appendix II: Questionnaire

The goal of this questionnaire is to collect information on CBK GCPSP on cyber security as a tool for ensuring safety in online banking transactions. You are kindly asked to respond to the questions as directed. As stated in the introductory letter, this information is kept strictly confidential and used solely for academic purposes.

Kindly tick inside the box where appropriate

SECTION A: DEMOGRAPHIC CHARACTERISTICS

1. Kindly indicate your Gender

Male [ ] Female [ ]

3. Please indicate your highest level of education.

Doctorate Degree [ ]

Master Degree [ ]

Bachelor's Degree [ ]

Diploma Certificate [ ]

4. Kindly indicate your professional certification

CFE [ ]

CFA [ ]

CPA [ ]

ACCA [ ]

None of the above [ ]

6. Kindly indicate the number of years of Professional Experience

1–5 Years [ ]

6– 10 [ ]

11 – 15 [ ]

16 – 20 [ ]

Over 20 [ ]

Section B: Access Control Measures and Security of Online Banking Transactions

The following statements relate to the effect of access control measures on the security of online banking transactions in the Kenya commercial banks. Please indicate your level of agreement with each of the statements as applicable to your bank.

Use a scale of 1 to 5, where (1 - strongly disagree, 2 -disagree, 3- not sure, 4 -agree and 5- strongly agree).

Statement	**1**	**2**	**3**	**4**	**5**
1. The security measures in place provide strong protection for online banking transactions					
2. I feel that access control measures effectively prevent unauthorized access to online banking accounts					
3. My confidence in the security of online banking transactions is high due to the controls my bank has implemented					
4. Security controls in my bank are reliable and reduce the likelihood of fraud in online banking					
5. The bank's access control systems make customers feel safe when performing online transactions					
6. Access control measures in online banking are user-friendly and do not create unnecessary difficulties for customers					
7. The bank's security measures provide comprehensive protection for clients' personal and financial information.					

Section C: Incidence Response and Security of Online Banking Transactions

The following statements relate to the effect of incidence response on the security of online banking transactions in the Kenya commercial banks. Please indicate your level of agreement with

each of the statements as applicable to your bank. **Use a scale of 1 to 5, were (1 - strongly disagree, 2 -disagree, 3- not sure, 4 -agree and 5- strongly agree).**

Statement	1	2	3	4	5
1. Our bank has a well-defined incident response plan for online banking security breaches					
2. The incident response procedures are regularly tested and updated to handle new security threats					
3. Online banking security breaches are effectively managed and mitigated by the bank					
4. The bank ensures prompt communication with customers in case of a security incident					
5. I feel confident that online banking transactions are secure due to the incident response plan.					
6. The bank's online banking platform is regularly tested for vulnerabilities.					

Section D: Data Protection Protocols and Security of Online Banking Transactions

The following statements relate to the effect of Data Protection and Encryption Protocols measures on the security of online banking transactions in the Kenya commercial banks. Please indicate your

level of agreement with each of the statements as applicable to your bank. **Use a scale of 1 to 5, where (1 - strongly disagree, 2 -disagree, 3- not sure, 4 -agree and 5- strongly agree)**

Statement	**1**	**2**	**3**	**4**	**5**
1. The data protection policies in place effectively safeguard customer information					
2. The encryption protocols used by our bank adequately protect sensitive data from unauthorized access					
3. Our systems prevent data breaches and protect customer data effectively					
4. Staff training on data protection and encryption protocols is sufficient for us to handle sensitive information responsibly					
5. Our bank regularly updates their data protection and encryption protocols to adapt to emerging threats					
6. My bank takes adequate measures to comply with relevant data protection regulations					
7. Data protection and encryption measures contribute to customer trust in our banking services					

Section E: Network Security Standards and Security of Online Banking Transactions

The following statements relate to the effect of network security standards measures on the security of online banking transactions in the Kenya commercial banks. Please indicate your level of agreement with each of the statements as applicable to your bank. **Use a scale of 1 to 5, where (1- strongly disagree, 2 -disagree, 3- not sure, 4 -agree and 5- strongly agree)**

Statement	**1**	**2**	**3**	**4**	**5**
1. The network security standards in place effectively protect online banking transactions from cyber threats					
2. Our bank's network infrastructure is robust enough to handle potential security breaches.					
3. Regular updates to network security protocols enhance the safety of online banking transactions					
4. Staff training on network security standards is sufficient to mitigate risks associated with online banking					
5. The bank's network security measures prevent unauthorized access to sensitive customer information					
6. The bank implements industry best practices for network					

security to ensure the safety of online transactions					
7. The network security standards contribute to customer confidence in using online banking services					
8. The bank has protocols to quickly address any security breaches that may occur in online transactions					

Section F: Institutional Resources

The following statements relate to the effect of institutional resources on the relationship between the CBK GCPSP implementation and security of online banking transactions in commercial banks in Kenya. Please indicate your level of agreement with each of the statements as applicable to your bank. **Use a scale of 1 to 5, where (1 - strongly disagree, 2 -disagree, 3- not sure, 4 -agree and 5- strongly agree)**

Statement	**1**	**2**	**3**	**4**	**5**
1. Financial resources are adequately allocated to implement CBK GCPSP for secure online banking transactions					
2. The technological infrastructure in the bank is sufficient to support the secure implementation of CBK GCPSP					

3. The bank has enough human capital with the necessary skills to effectively implement the CBK GCPSP					
4. The bank regularly invests in upgrading their technological infrastructure to ensure it can meet cyber security requirements					
5. Financial resources are prioritized for cyber security initiatives within the bank					
6. The bank provides adequate training and development programs for their staff to stay updated on cyber security trends and practices					
7. The bank has established a dedicated cyber security team to ensure the implementation of CBK GCPSP.					

Section G: Security of Online Banking Transactions

The following statements relate to security of online banking transactions in commercial banks in Kenya. Please indicate your level of agreement with each of the statements as applicable to your bank. Use a scale of 1 to 5, where (1 - strongly disagree, 2 -disagree, 3- not sure, 4 -agree and 5- strongly agree)

Statement	1	2	3	4	5
1. My bank provides secure login features (e.g., two-factor authentication) for online banking					
2. I feel confident that my personal and financial information is protected					
3. My bank frequently updates its security features to prevent cyber threats					
4. I have never experienced unauthorized access or suspicious activity on my online banking account					
5. I receive timely alerts from my bank for all transactions carried out online					
6. My bank educates customers on safe practices for online banking (e.g., avoiding phishing scams).					
7. I trust the encryption and data protection mechanisms used by my bank					

Appendix III: NACOSTI

REPUBLIC OF KENYA

NATIONAL COMMISSION FO
SCIENCE,TECHNOLOGY & INNOVATIO

Ref No: **199136**

Date of Issue: **15 /April**

RESEARCH LICENSE

This is to Certify that Miss.. LOICE WACHUKA NJUGUNA of Strathmore University, has been licensed to c per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: AN THE IMPLEMENTATION AND EFFECTIVENESS OF CBK CYBERSECURITY GUIDELINES FOR COM BANKS: THE MEDIATING ROLE OF INSTITUTIONAL RESOURCES. AN ASSESSMENT OF THE IMP AND EFFECTIVENESS OF CBK CYBERSECURITY GUIDELINES FOR COMMERCIAL BANKS: THE I ROLE OF INSTITUTIONAL RESOURCES. for the period ending : 15/April/2026.

License No: **NACOSTI/P/25/4172904**

199136

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY &
INNOVATION

Verification QR Code

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013 (Rev. 2014)

Legal Notice No. 108: The Science, Technology and Innovation (Research Licensing) Regulations, 2014

The National Commission for Science, Technology and Innovation, hereafter referred to as the Commission, was the established under the Science, Technology and Innovation Act 2013 (Revised 2014) herein after referred to as the Act. The objective of the Commission shall be to regulate and assure quality in the science, technology and innovation sector and advise the Government in matters related thereto.

CONDITIONS OF THE RESEARCH LICENSE

1. The License is granted subject to provisions of the Constitution of Kenya, the Science, Technology and Innovation Act, and other relevant laws, policies and regulations. Accordingly, the licensee shall adhere to such procedures, standards, code of ethics and guidelines as may be prescribed by regulations made under the Act, or prescribed by provisions of International treaties of which Kenya is a signatory to.
2. The research and its related activities as well as outcomes shall be beneficial to the country and shall not in any way; i. Endanger national security
    ii. Adversely affect the lives of Kenyans
    iii. Be in contravention of Kenya's international obligations including Biological Weapons Convention (BWC), Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO), Chemical, Biological, Radiological and Nuclear (CBRN).
    iv. Result in exploitation of intellectual property rights of communities in Kenya
    v. Adversely affect the environment
    vi. Adversely affect the rights of communities
    vii. Endanger public safety and national cohesion
    viii. Plagiarize someone else's work
3. The License is valid for the proposed research, location and specified period.
4. Neither the license nor any rights thereunder are transferable.
5. The Commission reserves the right to cancel the research at any time during the research period if in the opinion of the Commission the research is not implemented in conformity with the provisions of the Act or any other written law.
6. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research.
7. Excavation, filming, movement, and collection of specimens are subject to further necessary clearance from relevant Government Agencies.
8. The License does not give authority to transfer research materials.
9. The Commission may monitor and evaluate the licensed research project for the purpose of assessing and evaluating compliance with the conditions of the License.

10. The Licensee shall submit one hard copy, and upload a soft copy of their final report (thesis) onto a platform designated by the Commission within one year of completion of the research.
11. The Commission reserves the right to modify the conditions of the License including cancellation without prior notice.
12. Research, findings and information regarding research systems shall be stored or disseminated, utilized or applied in such a manner as may be prescribed by the Commission from time to time.
13. The Licensee shall disclose to the Commission, the relevant Institutional Scientific and Ethical Review Committee, and the relevant national agencies any inventions and discoveries that are of National strategic importance.
14. The Commission shall have powers to acquire from any person the right in, or to, any scientific innovation, invention or patent of strategic importance to the country.
15. Relevant Institutional Scientific and Ethical Review Committee shall monitor and evaluate the research periodically, and make a report of its findings to the Commission for necessary action.

National Commission for Science, Technology and Innovation(NACOSTI),
Off Waiyaki Way, Upper Kabete,
P. O. Box 30623 - 00100 Nairobi, KENYA
Telephone: 020 4007000, 0713788787, 0735404245
E-mail: dg@nacosti.go.ke
Website: www.nacosti.go.ke

Appendix IV: Ethical Review

Strathmore UNIVERSITY

30th March 2025

Mr. Loice Wachuka,
loice.njuguna@strathmore.edu

Dear Miss Loice,

RE: An Assessment of the Implementation and Effectiveness of CBK Cybersecurity Guidelines for Commercial Banks: The Mediating Role of Institutional Resources.

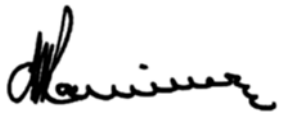
This is to inform you that SU-ISERC has reviewed and approved your above SU-master's proposal. Your application reference number is SU-ISERC2817/25. The approval period is from 27th March 2025 to 26th March 2026.

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU- ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions. vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU- ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research- portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,



Mr Ambrose Rachier, Chairperson; SU-ISERC

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000

Email admissions@strathmore.edu www.strathmore.edu