ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

Investigating the Challenges and Best Practices for Implementing Cybersecurity Frameworks and Policies in the Banking Sector in Sierra Leone

Oludolapo O. Akinyosoye–Gbonda[1]; Augustine Sessie[2]; Alhaji Samura[3]; Hannah Bangalie[4]

[1](Ph.D.)
[1.2.3.4] Department of Information Technology, Institute of Public Administration and Management - University of Sierra Leone

Publication Date: 2026/02/16

Abstract: Cybersecurity is a critical concern for Sierra Leone's banking sector due to increasing digitalisation and cyber threats. The study aimed at investigating the challenges and identify best practices for implementing cybersecurity frameworks and policies within commercial banks in Freetown's Western Area Urban, with a focus on enhancing information system security. The research employed a mixed-method approach, combining quantitative surveys questionnaire and qualitative interviews involving bank staff, IT personnel, managers, regulators, and customers. Key findings reveal significant gaps between policy awareness and implementation, compounded by outdated systems, insufficient funding, skill shortages, and weak regulatory enforcement. Based on the findings, the study recommends the adoption of context-sensitive cybersecurity frameworks, coupled with regular training programs and investment in modern security technologies. Additionally, stronger collaboration between banks, regulators, and customers is essential to build a resilient cybersecurity culture. These measures are vital for safeguarding financial data, ensuring service continuity, and promoting trust in Sierra Leone's evolving digital banking landscape.

Keywords: *Cybersecurity, Banking Sector, Sierra Leone, Cyber Threats, IT Personnel Regulators.*

How to Cite: Oludolapo O. Akinyosoye–Gbonda; Augustine Sessie; Alhaji Samura; Hannah Bangalie (2026) Investigating the Challenges and Best Practices for Implementing Cybersecurity Frameworks and Policies in the Banking Sector in Sierra Leone. *International Journal of Innovative Science and Research Technology*, 11(2), 631-642. https://doi.org/10.38124/ijisrt/26feb405

I. INTRODUCTION

Cybersecurity has become an increasingly critical issue in the banking sector due to the escalating threat of cyber-attacks. The objective of this research is to investigate the challenges and identify best practices for implementing cybersecurity frameworks and policies in banks in Freetown, with the aim of enhancing the security and resilience of their information systems.

The Sierra Leone banking industry plays a vital role in ensuring national economic stability since they handle sensitive financial data and foster public service. In Freetown, Western Area Urban in the middle of the country's financial system, banks rely greatly on technology like core banking platforms and mobile/online services to deliver more convenient, efficient and quicker services to their customers. And with the growing resilience on digital solutions are greater exposure to cyber-attacks in the disguise of data breaches, ransom ware, phishing attack, denial of service and financial fraud. The growing digitalization of Sierra Leone banking sector as a desirable trend has brought new risk that still tests many institution's infrastructure, competence capacity to manage these emerging trends and technologies (Kamara, 2019).

For example, a national commercial bank, one of the largest and leading banks in the country, has embraced technology by introducing mobile apps, online banking platforms and their online services for Urban and rural clients alike. However, this expansion and innovation have also placed them at risk of more cyber threats and attacks. Phishing attacks on customer's data increase by 37% in 2023 according to the national commercial bank records. This is a trend on the increase in developing countries where banks are at risk of increase cyber-attacks such as ransom ware attacks, data breaches and Advanced Persistent Threats (APTs).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

An advanced Persistent Threat (APTs) is a prolonged and targeted cyber-attack where an attacker has access into a network and remains undetected for a long time. APTs are often carried out by highly skilled attackers, including state-sponsored attackers, with the motive of gaining sensitive information rather than causing immediate damage (Kawimbe & Kwalombota, 2024). World renowned cyber security frameworks like National Institute of Standards and Technology (NIST) and International Organization for standardization (ISO 27001) together with the national cybersecurity law of Sierra Leone offers blueprints to mitigate risks, but their implementation in Sierra Leone is uneven. The national commercial bank's implementation of ISO 27001 in 2022 reveals exceeding vulnerabilities: outdated legacy systems trailing behind, uneven staff training, resistance to change, and budgeting limitations hindering advanced security tools. This study analyzes these issues through the example of the national commercial bank, finding cyber resilience impediments in Freetown's banking sector.

Sierra Leone's banking sector is particularly vulnerable to cyber-attacks with the intent of compromising confidentiality, integrity and availability, siphoning off citizens data, or interrupting vital public service. As much as established cybersecurity standards are formally adopted, the majority of banks are facing significant implementation gaps that expose their information systems. Uncertain banking structures, scarcity of trained and qualify personnel, lack of finance to enhance those bank's information systems divisions, and resistance to change from the bank and of course, its clients are the main explanations for these deviations. The following are the vulnerabilities of the information systems of the banking sector - Structural shortcomings: Fragmented regulatory oversight and antiquated IT infrastructure; Shortages of human resources: Core lack of trained cybersecurity staff; Constraints of resources: Insufficient funding for information system modernization; and Cultural resistance: Resistance from bank staff members and customers to adopt security standards.

These vulnerabilities make such systems as those used in handling transactions and storing customers' data more vulnerable to cyber-attacks. These attacks would cause grave problems, including sabotaging the services of banks, exposing people's personal details, and even affecting the nation's economy. Freetown Western Area Urban banks, without cybersecurity that is tailored to suit the local environment, are still not adequately prepared to deal with rising threats.

II. MATERIALS AND METHODS

The digitisation of banking services in Sierra Leone has accelerated financial inclusion and operational efficiency but introduced significant cybersecurity vulnerabilities. As cyber threats evolve globally, Sierra Leone's banking sector faces unique challenges shaped by its regulatory landscape, technical infrastructure, and socioeconomic context. This review synthesizes current research on cybersecurity frameworks, threat landscapes, implementation barriers, and best practices specific to Sierra Leone, drawing on local studies and comparative analyses.

❖ *Review of Literature*

➢ *Cybersecurity in the Modern Digital Landscape*

The digital world has grown rapidly, changing how we interact with each other, organisations, and countries. While this connected world offers many opportunities, it also introduces complex cyber threats. As more critical systems move online and cloud technology becomes standard, cybersecurity is crucial for protecting digital structures.

Cyber threats are evolving quickly, and hackers use tools like malware, ransomware, phishing, and advanced persistent threats (APTs) to exploit vulnerabilities in connected systems. These attacks can target anyone, from individuals to nations, and cybercriminals' goals can range from financial gain to political motivations.
To combat these threats, security solutions must constantly adapt. This study will explore cybersecurity frameworks and methods used to protect banking systems, focusing on:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2020); and
- International Organisation for Standardisation (ISO 27001, 2013).

These frameworks provide guidance on identifying vulnerabilities, implementing protections, and detecting threats. This research discusses their components, benefits, and impact on risk management.

By understanding how these frameworks work, this research can better help banking sectors secure their Information systems and protect against cyber threats.

➢ *The Status of Cybersecurity in the Banking Sector Across the World*

The shift to digital banking has transformed the way banks operate bringing greater efficiency, broader access, and a global reach that was once unimaginable. But with this progress comes a new wave of challenges. Cybersecurity threats have become increasingly common and complex, especially in developing countries where the technology and regulatory systems are still catching up (Girling, 2022; Saeed et al., 2023).

To guard against these risks, many banks rely on well-established cybersecurity frameworks such as the National Institute of Standards Technology (NIST) Cybersecurity Framework and ISO/IEC 27001. These standards help institutions manage risks like phishing, ransomware, and data breaches by promoting proactive planning, regulatory compliance, and continuous system improvement (Dawodu et al., 2023; Sulistyowati et al., 2023). However, in places like Sierra Leone, putting these frameworks into practice is not always easy. Limited resources, fragmented oversight, and gaps in technical capacity make it harder for banks to protect their systems effectively.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

As highlighted by British Bankers Association (BBA) and Pricewaterhouse Coopers (PwC) (2014), cyber threats have become a global issue, demanding strategic responses tailored to each context. In many banks, the responsibility for cybersecurity is scattered across different departments, which can create confusion about where threats are coming from and how best to respond (Al-Alawi, Al-Bassam & Mehrotra, 2020). The most serious intrusions can compromise entire systems—stealing, altering, or even destroying sensitive data. Hackers often exploit weaknesses in software, hardware, or even human behavior, causing damage that goes far beyond just the financial loss. These attacks can shake public trust, destabilise markets, and affect investor confidence through fluctuations in share prices.

As Summerfield (2014) pointed out, the impact of digital technologies on banking is both profound and double-edged. While they open up new opportunities for innovation and customer engagement, they also bring new vulnerabilities that banks must be ready to address with urgency, coordination, and context-aware solutions.

Today's financial institutions rely heavily on third-party providers for the digital tools and technologies that power their day-to-day operations. To stay efficient and competitive, many banks have embraced technological upgrades that make transactions faster and more convenient. But while these advancements bring clear benefits, they also come with serious risks, particularly in the form of cybercrime, which has been on the rise. Summerfield (2014) reported that even the world's top 50 banks have faced cyber-attacks on their websites, resulting in staggering annual losses of around $1 billion. This highlights a growing reality: cybersecurity is no longer just an Information Technology issue it's becoming a competitive edge. In an era where customer trust is tied to data protection, banks that invest in stronger security systems stand to gain a loyal customer base. Cawley (2017) notes that the banking industry is struggling to keep up with the rapid pace of technological innovation, especially when it comes to aligning these changes with operational regulations. Many banks are also burdened with outdated systems so-called "technological inheritance" that poses both usability challenges and serious security risks for clients.

One example of a protective measure is two-factor authentication (2FA), which adds an extra layer of security by sending a code to a user's phone before granting access to their account. This means that even if a hacker gets hold of a customer's login credentials, they would also need access to their mobile device. However, despite its effectiveness, many banks still do not use 2FA, leaving client accounts more vulnerable than necessary.

In a world of evolving digital threats, the gap between innovation and protection must be closed not just for operational success, but for customer safety and long-term trust. He explained the situation in a Bangladeshi bank, which has vulnerabilities within the computer system of the bank. They detected malware in the customer computer system; attackers use this malware to bypass risk controls and start the process of transferring funds. Kuepper (2017) argued that clients experience low losses from banking cyber-attacks because they would quickly respond to missing funds by informing the bank. In the USA, the law requires banks to refund the client in the case of theft of funds from their account without their authorisation, in the case where the client has notified the bank of the loss within 60 days of the transaction. McGoogan (2017) indicated in The Telegraph that the fraud of financial Cyber-attacks against banking and financial services institution cost end-users more than $10.5bn in 2016, and it increased by 122% from the previous year. Online transactions increased by 10% for the same period. Therefore, the online creditors are under intensifying stress to implement stronger and smarter authentication mechanisms to accelerate authentic and proper loans and terminate fraud. These are some of the arguments from different experts regarding status of cybersecurity in the banking sector worldwide.

➢ *Cybersecurity Framework Basics*

Cybersecurity framework therefore refers to a framework which comprises of principles, practices and standards that organisations use to protect their information systems, networks and data from cybersecurity threats. These frameworks prevent the creation of cybersecurity approaches that are non-systematic, non-iterative, and can't be successfully replicated – which is precisely what's needed for a rapidly evolving threat landscape in computer crime. The need for cybersecurity frameworks in the banking sector is anchored in the fact that they help banks create a level of uniformity and reduce all risks derived from cyber risks. Through instrumentalist, these frameworks provide structures for those banks to put in place security measures that will be in line with the set standard, minimise risks that might lead to a cyber-attack and improve resilience in the case of an attack.

- Key Reasons for Adopting Cybersecurity Frameworks – are for Consistency: frameworks are designed to make sure all implements of security are similar for all the different systems and processes of the business making it have a coherent security structure; for Risk Management: they enable banks to consider the risks and make appropriate decisions on the allocation of funds to avert the highest risks to the business; for Compliance: most of the cybersecurity frameworks reflect legal and regulatory standards, as well as industry standards, thus helping banks meet cybersecurity standards within their legal environment; and for Continuous Improvement: frameworks contain procedures for assessing and reviewing security controls as well as recommending updates and improvements to bank's security systems in response to emerging threats.

➢ *Frameworks as a Foundation for Consistent and Proactive Cybersecurity*

Frameworks of cybersecurity help applicable banks to have the working tools which enable them to undertake coherent and preventive security measures. These frameworks provide a starting point for banks to build a strong cybersecurity framework, which will apply universally across their operations Trade-offs for specific activities, can

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

then be made consistently with the bank's overall cybersecurity posture. (Dawadu, 2023)

- Proactive Threat Mitigation: Zero Threat Architecture (ZTA) has brought up the principles of continuous user and device verification meaning there is no pre-trusted identity and that all the identities' access request should be validated upfront.

- Data Protection and Monitoring: Frameworks also highlight the importance of ratification and dataveillance referring to the presence of big data and surveillance methods throughout cybersecurity mentioning live threat monitoring and identification. Risk control is an important part of data governance that makes use of data analytics together with ongoing monitoring in the identification of possible risk openings that further extend to becoming risk threats waiting to be leveraged by the attackers within the banking sector. (Gramavikle, 2023)

Also. frameworks such as the National Online Informative References (OLIR) program are other approaches that ensure that banks are provided with consistent forms of information that they can work with to enhance their cybersecurity by providing informative references that organizations follow in regards to cybersecurity and that update them on new and more threatening risks or complex solutions regularly.

These sources help cybersecurity professionals to get updated information related to security frameworks that will help them protect their organizations' critical assets from the contemporary threats more effectively.

These cybersecurity frameworks when adopted and implemented ensure that banks have security-first approach to any project, so that risks are constantly assessed, and controls are observed to deter cybersecurity incidents. This is particularly important in the current world where new forms of threats appear constantly, and their complexity increases.

➢ *Popular Cybersecurity Frameworks and Policies*

Given the rapidly changing nature of cyber threats, organising for security needs to have systematic approaches for addressing problems and prospects. Both of these frameworks are also useful to assist in other areas than merely protecting digital assets, but explaining how to create strong cybersecurity defense. Jointly with that, below is the comprehensive analysis of several of the most popular cybersecurity frameworks in terms of the main concepts and practices.

- National Institute of Standards Technology (NIST) Cybersecurity Framework - the NIST Cybersecurity Framework (CSF) is the NIST framework that has proven popular and sought after, which enables banks to improve in cybersecurity. Originally developed for identifying the critical infrastructure, the NIST being extensible, customisable and compliant with present standards, has been implemented in other sectors as well.

The National Institute of Standards Technology (NIST) CSF is built around five core functions:

- Identify: The first function centers on coming up with an assessment of the organisation's cybersecurity exposure. This involves the process of listing those that involve the banks' assets, system, data or resources that requires protection. Risk identification process enables the development of a framework within which risks and threats will be managed.
- Protect: This function defines all the required safeguards for safeguarding the key assets from risks in the future. These are such issues as maintenance of sound access control measures, data encryption, frequent patching as well as security measures against malware and unauthorised access.
- Detect: It requires constant and active scanning and detection in order to detect that an incident or intrusion is occurring in real-time. In this function, concern is given more on the development of detectors in a view to be able to detect some of these anomalies, intrusions, and any other form of malice.
- Respond: Controlling the impact of cybersecurity incidents requires having the right strategies for managing incidents. This function addresses how organisations should protect against 'inside' threats, and what to do if an incident is discovered, how the event should be handled and explained; how organisations should limit the consequences of a security breach.
- Recover: The last function in the National Institute of Standards Technology (NIST CSF) relate to recovery activities in order to bring back the functionality that was affected by a cybersecurity threat. This consists of disaster responses and continuity of services through the planning of continuation in case of disruptive incidents, and also the creation of backups in case of service interruption. The National Institute of Standards Technology (NIST) basically provides an effective framework for managing cybersecurity risk at an organizational level with certain degree of flexibility in terms of risk appetite and strategies and goals of the particular organization that is implementing the risk management process. Its compatibility with other Industry standards like International Organisation for Standardisation (ISO/ 27001) and regulatory frameworks like General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) lays it as a golden framework which can be adopted as per the industry's need and size.

- Control Objectives for Information and Related Technologies (COBIT) - COBIT, developed by ISACA (Information Systems Audit and Control Association), is a comprehensive framework designed for Information Systems governance and management. Unlike purely technical cybersecurity standards, COBIT emphasizes the alignment of Information technology goals including cyber security with broader organisational and business objectives. It serves as a bridge between technical capabilities and strategic enterprise needs, making it

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

especially relevant to sectors like banking where regulatory compliance, data integrity, and operational efficiency are paramount.

At its core, COBIT provides a structured approach to managing and governing enterprise Information systems. The framework is divided into two key domains - Governance: The governance component focuses on evaluating stakeholder needs, setting direction, and monitoring performance; and Management Domain: This is concerned with planning, building, running, and monitoring information system processes. This distinction helps institutions like banks maintain accountability and ensure that Information System resources, including cybersecurity mechanisms and polices, are effectively aligned with business goals. (Summerfiled, 2023).

(Summerfield, 2023) continued by saying, One of Control Objectives for Information and Related Technologies (COBITs) strengths lies in its performance measurement tools. These tools enable organisations especially banks to assess their cybersecurity maturity, identify gaps, and track improvements over time. Additionally, COBIT integrates with other frameworks such as International Organisation for Standardisation (ISO/IEC 27001) and Information Technology Infrastructure Library (ITIL), providing a harmonized environment for IT management. In the context of banking, this is vital, as institutions must constantly audit their systems for both security and regulatory compliance.

Furthermore, COBIT supports risk optimization by ensuring that cybersecurity investments align with actual business priorities. It encourages regular risk assessments and offers guidance on integrating Information Technology (IT) risk into broader enterprise risk management strategies. This makes COBIT particularly suitable for financial institutions, where poor IT governance can lead to operational failures, legal repercussions, or loss of customer trust.

In summary, COBIT is not just a technical framework; it is a governance tool that enhances decision-making at the intersection of business and IT. Its structured approach, performance tools, and focus on strategic alignment make it a powerful choice for banks aiming to strengthen their cybersecurity posture while fulfilling organisational and regulatory requirements.

- Zero Trust Architecture (ZTA) - Amidst contemporary cyberspace, Zero Trust Architecture (ZTA) differs as a state-of-the-art concept particularly useful in hybrid computing systems. The Zero Trust model postulates that there cannot be a trusted entity either internal or external to a network. This is a needed shift as perimeter-based security models have become more and more ineffective due to more work from home, cloud computing, and advanced hacking. The core principles of Zero Trust Architecture are: Never Trust, Always Verify: This principle supports constant affirmation of user identities, gadgets, and applications that intends to connect to the organisational resources. There needs to be authentication at every viewpoint, not only at the time of the login. The result is that nobody gets to work with the data without undergoing approval from other parties in the organisation; Least Privilege Access: Zero Trust is centered on the idea of least privilege where access is granted to the barest minimum needed for the user and his device. This is important in order to avoid a corrupted entity getting access to information or networks of an organization; Micro-Segmentation: Exemplary of the Zero Trust model, the network is broken down into various compartments, so that an attacker who is able to breach one particular compartment cannot easily move to the next compartment. This segmentation reduces contact and keeps potential foe away; and Continuous Monitoring and Analytics: Monitoring of network traffic, users' actions, and system events is continuous because Zero Trust presupposes scanning for risks and threats. Instead of searching for known patterns, behavioral analytics and machine learning are utilized to identify scheduling that may suggest a breach is taking place. Zero Trust works well when implemented in counteract to insider attacks and the new generation of attacks including spear phishing, lateral movement and data extraction. The primary set of principles of the zero.

Trust model is identity and access management (IAM), encryption, and real-time monitoring, which makes it better suited for the modern context where the threats can be more diverse and harder to predict than in traditional, closed environments, such as those promoted by cloud computing and remote work principles.

➢ *Challenges and Gaps in Existing Cybersecurity Frameworks*

One of the identified issues is the lack of the single and the all-encompassing cybersecurity model, which could be implemented to the financial companies, especially the new generation Internet-based technology companies and the finch organisations. Frameworks like the National Institute of Standards Technology (NIST) Cybersecurity Framework are handy; however, they are better designed for mature and enterprise-style banks rather than the innovative and constantly evolving finch firms.

In the words of Goodwin (2022) there are many financial institutions that have no legally binding requirements for the execution of cybersecurity based on voluntarily adopted frameworks such as the NIST. It implies that, although some organisations can choose to adopt the best practice frameworks, others may not do the same; effectively giving the sector an uneven security position. In particular, differing paradigms combined with insufficient regulation in the sphere of finance increases the problem of protection from the new threats in the sphere of cybersecurity. Much more can be expected from the existing and forming regulatory structures to set and enforce cybersecurity requirements and measures.

Not only is there a great deal of regulatory ambiguity, there are also a lot of technological difficulties. The implementation of cloud services has myriad advantages in regard to flexibility and scalability, but where important

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

financial data is stored in public or hybrid cloud environments; there are unique and considerable risks. According to Desai & Hamid (2021), safety measures should be implemented in relation to cloud security; thus, it should meet industry requirements. The issue is how to deal with the risks which are linked to the usage of cloud technologies, and how to take the benefits which are offered by these technologies, at a lower cost and with greater flexibility.

➢ *Evolving Cybersecurity Threats in the Banking Sector*

The threat environment in the banking industry is dynamically changing, and this process is promoted by the following factors: technological progress, the growth of connecting societies, and complication of cyber threats. Writing for CSO, Marican et al. (2022) note that there are instances of cyberattacks on technology startups and especially those in the financial technology industry because they do not have well-developed cybersecurity frameworks as is the case with well-established in the banking institutions. The lack of a broad cybersecurity maturity model for technology startups only worsens the situation in this segment of the financial industry. Sometimes, startup companies may lack the necessary resources and experience to protect them from today's complex cyber threats, as many of them are driven by the concept of high growth rates and product Innovation.

The literature review conducted by Jain et al. (2023) comes to the conclusion that the transition from traditional types of crimes to cybercrimes is a characteristic feature of the present state of affairs in the field of finance cyber-safety. This shift can be linked to financial technology from mobile apps and the now famous financial tools such as Block chain and AI services. These generally are new technologies that are creating new and improved ways whereby the hackers can gain access to the systems' vulnerabilities, always at a pace that is much faster than the speed at which even legislation and existing security measures can evolve adequately. This is explained by the fact that for some reason technological change is continuing at a much faster pace than our rules and even laws that, more often than not, are unable to respond to the new threats that flow from such developments as noted by Jain et al. Furthermore, insider threat remains a very influential threat within the financial area. As observed by (Marican, 2022) insider abuse is a common type of account abuse that can result to high levels of financial and reputational loss. This is because organisations are susceptible to any wrong deeds from any of their personnel who have access to the information or systems of an organisation. These are a threat hard to notice and prevent, meaning financial institutions need to enforce a set of internal controls, security procedures and monitoring, and staff training to avoid risks within the banking sector.

➢ *Current Cybersecurity Practices in Sierra Leone's Banking Sector*

Sierra Leone's cyberspace is increasingly targeted by both opportunistic and sophisticated attacks: Rising Cybercrime: Sawaneh (2018) documented prevalent threats including phishing, SIM boxing (telecom fraud), and identity theft, exacerbated by limited public awareness and weak legal frameworks. Financial losses from cyber fraud exceeded $2 million USD in 2022 (Bank of Sierra Leone, 2023). Critical Infrastructure Vulnerabilities: Banks face Advanced Persistent Threats (APTs) targeting core banking systems, with 65% of Sierra Leonean banks reporting at least one major breach between 2020–2023 (Sawana, 2023). Data Protection Gaps: Sensitive customer data is inadequately encrypted, and incident response protocols are underdeveloped, leaving banks exposed to ransomware (Sawaneh, 2018).

Sierra Leone's banking sector has made progress in cybersecurity, driven by the Cybersecurity and Crime Act of 2021. This act established the National Cybersecurity Coordination Centre (NC3), which plays a pivotal role in managing cybersecurity incidents. The NC3 has implemented capacity-building initiatives, including training workshops and symposiums, to enhance cybersecurity awareness and skills among stakeholders Kamara, (2022).

(Kamara, 2023) said that there are key initiatives that should be implemented within the banking sector in Sierra Leone, namely the National Cybersecurity Coordination Centre (NC3): Provides strategic leadership and oversight on cybersecurity implementation and development; Capacity Building: Training programs for staff, law enforcement agencies, and judiciary to enhance cybersecurity expertise; and Collaboration: Partnerships with international organizations, such as the World Bank, to support digital transformation and infrastructure development.

➢ *Regulatory and Institutional Frameworks*

Sierra Leone's cybersecurity governance remains fragmented by Weak Legislation: No dedicated cybercrime law existed until the draft Cybersecurity and Cybercrime Act (2023). Existing regulations rely on the National Telecommunications Commission (NATCOM), which lacks enforcement capacity Sawaneh, (2018); Institutional Challenges: The Cyber Security Unit (CSU) of the Sierra Leone Police and the Office of National Security (ONS) suffer from shortages of skilled personnel and forensic tools. Sawaneh (2018) noted that 70% of staff in these units had no formal cybersecurity training; and Compliance Gaps: Only 30% of banks fully adhere to international frameworks like ISO 27001 or National Institute of Standards Technology (NIST CSF) due to resource constraints and ambiguous national standards Sawaneh, (2025).

- Challenges Preventing Effective Implementation - Adopting cybersecurity frameworks faces systemic barriers: Kamara, (2023) continued to give further reasons why Sierra Leone is striving to implement cybersecurity frameworks within the banking industry.

He said despite progress, Sierra Leone's banking sector faces challenges in implementing effective cybersecurity measures. These include:

- Limited Expertise: Initial lack of specialized knowledge in cybersecurity and cyber law.
- Resource Constraints: Insufficient funding and technological infrastructure hinder effective

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

implementation. 60% of banks cite insufficient budgets for cybersecurity upgrades, prioritising customer-facing digital services over security hardening (Kawimbe & Kwalombota, 2024).

- Public Awareness: Limited understanding of cybersecurity risks and best practices among the general public.
- Technical Infrastructure: Legacy systems dominate 80% of banks' IT environments, hindering integration with modern security tools (e.g., AI-driven threat detection) Sawana, (2025).
- Human Capital Shortages: A critical skills gap persists, with fewer than 50 certified cybersecurity professionals nationwide Sawaneh, 2018). Staff training is often theoretical rather than hands-on, reducing preparedness.
- Cultural Resistance: Employees and customers resist security protocols (e.g., multi-factor authentication), perceiving them as cumbersome Sawaneh, (2024).

- Developing a Context-Sensitive Framework for Cybersecurity – in developing a context-sensitive framework, consider the following: Assess Local Threats - Identify specific cybersecurity threats and vulnerabilities in Sierra Leone's banking sector; Regulatory Compliance: Ensure compliance with local regulations and international standards; Stakeholder Engagement: Collaborate with banks, government agencies, and international partners to develop a comprehensive framework; and Capacity Building: Invest in training and capacity-building programs for cybersecurity professionals.

➢ *Case Study Insights from Zambia*

The Zambian banking sector's digitisation highlights challenges mirroring those in Sierra Leone. A mixed-methods study of 123 banking professionals revealed critical vulnerabilities, including outdated software, insufficient employee training, and weak encryption protocols (Kawimbe & Kwalombota, 2024). Over 47% of respondents lacked specialized cybersecurity training, while 23.6% rated incident response plans as "very ineffective." Recommendations emphasise regulatory compliance, secure software development, and vendor risk management key areas for Sierra Leone to address.

- Comparative Insights from other African countries -Sierra Leone can learn from regional experiences: Ghana and Nigeria: Implemented mandatory cybersecurity frameworks for banks, reducing breaches by 40% through centralized threat-sharing platforms (Kawimbe & Kwalombota, 2024). Zambia's Model: Regular security audits and public-private partnerships improved incident response times by 50%. Employee training reduced phishing success rates by 35% (Kawimbe & Kwalombota, 2024).

➢ *Methods for Effective Cybersecurity Policy Implementation within the Banking Sector in Freetown Western Area Urban*

Effective implementation requires:

- Integrated Compliance Programs: Streamline compliance efforts and reduce redundancy.
- Automated Compliance Tools: Utilize technology to manage compliance tasks and improve efficiency.
- Regular Audits and Training: Conduct regular audits and training programs to ensure compliance and awareness.
- Incident Response Planning: Develop comprehensive incident response plans to quickly respond to cybersecurity incidents. (Sawaneh, 2024)

- Cyber Security Best Practices for Sierra Leone's Banking Sector to Adopt - The increasing reliance on digital technologies has led to a surge in cyber threats with the banking sector, compromising the security and integrity of banks data and systems. Implementing effective cyber security best practices is crucial to mitigate these threats in Sierra Leone Banking Sector. From existing research on cyber security, best practices to inform banks and individuals on strategies to enhance their security posture include:

- Contextualised Frameworks - Adapting National Institute of Standards Technology (NIST/ISO) 27001 to Sierra Leone's infrastructure constraints, emphasising cost-effective controls like encryption and access management to enhance save transaction now that banks are embracing the Salone Payment Switch (Sawana, 2025).

➢ *Adoption of Best Practices*

- Human-Centric Approaches - As we strive to create solutions that truly makes a difference, it's essential to follow the necessary approaches. Practical Training: Simulations of phishing/ransomware attacks boost staff responsiveness (Cryer & Zounlome, 2018); Awareness Campaigns: Public education reduces social engineering risks (Sawaneh, 2018); and Regular Staff Training: Enhancing employees' awareness of cybersecurity threats (Obi et al., 2024). Employee education and awareness are vital components of cyber security. Training programs can significantly reduce the risk of phishing and social engineering attacks (Kumaraguru et al., 2007). Encouraging a culture of security within banks can promotes vigilance and responsible behavior among employees.

- Technology Integration - Technology integration includes: AI-Driven Solutions - real-time anomaly detection systems reduced false positives by 60% in Nigerian banks (Kawimbe & Kwalombota, 2024); Secure System Development Life Cycle (SDLC): Embedding security in software development prevents vulnerabilities in digital banking apps (Khan & Malaika, 2021); and Investment in Advanced Technologies: Utilizing AI and other technologies to detect and respond to threats (Shoetan & Familoni, 2024).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

- Network Security - One fundamental best practice is to implement robust network security measures. According to a study by Khan et al. (2019), firewalls and intrusion detection/prevention systems (IDPS/IPS) are essential in preventing unauthorised access and detecting malicious activities. Regular software updates and patches also play a critical role in fixing vulnerabilities and preventing exploitation (Verizon, 2020).

- Authentication and Access Control - Implementing strong authentication and access control mechanisms is another critical best practice. Multi-factor authentication (MFA) significantly reduces the risk of unauthorised access (Bonneau et al., 2015). The principle of least privilege access, where users are granted only necessary permissions, also minimises potential damage from compromised accounts (Sandhu et al., 1996).

- Data Protection - Protecting sensitive data is paramount. Encryption, both in transit and at rest, ensures confidentiality and integrity (Rescorla, 2000). Regular backups and disaster recovery plans also enable banks to respond effectively to data breaches or losses (Wood et al., 2011).

- Regulatory Enhancement - In today's rapidly evolving landscape, to mitigate risk and promote compliance, key aspect of regulatory framework is:

✓ Stronger Laws: Enacting the Cybersecurity and Cybercrime Act with clear penalties for non-compliance.
✓ Cross-Border Collaboration: Sharing threat intelligence with Economic Community of West Africa State (ECOWAS) partners to combat transnational cybercrime (Kamara, 2023).
✓ Adoption of International Standards: Implementing frameworks like ISO 27001 to strengthen security posture (ISMS. online, 2025).

In conclusion, implementing cyber security best practices is essential to mitigate cyber threats. By focusing on network security, authentication and access control, data protection, awareness and employee education, banks can significantly enhance their security posture. Continuous monitoring and adaptation to emerging threats are also crucial in maintaining effective cyber security.

❖ *Research Methodology*

his survey was conducted over a 2-week period in Freetown, Western Area in October/November 2025 and targeted key stakeholders in Sierra Leone's banking sector, including IT staffs, banking managers, regulatory officials from a national commercial bank, an indigenous commercial bank and the National Cybersecurity Coordinating Centre etc., customers, staffs and cybersecurity consultants in Freetown, Western Area Urban.

A purposive sampling technique was be used to select participants for the qualitative phase, while a random sampling technique will be used for the quantitative phase. The sample size determined was based on the saturation point for qualitative data and statistical power analysis for quantitative data. A total of 170 questionnaires were sent through online google form; however, 130 respondents completed the questionnaires; the survey had a response rate of 76.5%.

The researchers conducted semi-structured interview with banking professionals and regulatory officials as respondent to gather qualitative data. A quantitative questionnaire was developed using online google form for quantitative data on current cybersecurity practices, technical controls, and incident response protocols; and documents on existing cybersecurity frameworks, policies and guidelines in Sierra Leone's banking sector were reviewed.

Data analysis involved the following Thematic analysis: For qualitative data, themes were used identified and analysed to understand current cybersecurity practices, challenges and potential solutions from respondents while Descriptive statistics were used to summarise and visualise the quantitative data to facilitate understanding and interpretations and inferential statistics will be used to identified relationships between variables.

III. FINDINGS AND DISCUSSIONS

A. Demographic Characteristics

Data were obtained from 130 respondents from the targeted stakeholders in the sector under review. The demographic factors revealed that there were more male 54.6% and female 45.4% for this study accounting for a significant proportion of the sample size, indicating a male-dominant workforce in the banking ecosystem. The predominance of male respondents could reflect broader industry trends, but it also highlights the need for inclusive training programs to ensure diverse voices contribute to cybersecurity strategies. The analysis revealed that bank staff and customers made up 77.7% (19.2% and 58.5%, respectively) of the respondents, while IT security personnel accounted for 11.5%. The sample also includes managerial and consulting perspectives, ensuring broad insights into cybersecurity practices. Bank Managers accounted for 7.7% which shows commitment in ensuring there is an interest in decisions made on cybersecurity related issues within the bank. Cybersecurity consultants, though fewer in percentage (3.1%), provided critical insights into user-end challenges. Bank respondents held various roles such as bank staff, IT security personnel, bank managers, and customers. This diversity ensures a broad understanding of cybersecurity perceptions and practices across the banking ecosystem. An IT professional commented: "Each role brings unique challenges. For instance, managers focus on budget constraints, while IT teams grapple with technical implementation gaps."

➢ *RQ1: What are the Current Cybersecurity Practices in Sierra Leone's Banking Sector?*

According to the analysis, the findings reveal the adoption of different standards like ISO/IEC 27001 as the main standard and gaps in operational effectiveness. The findings highlight critical areas for improvement to strengthen defences against evolving cyber threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

Stakeholder insights further underscore the need for standardised protocols and proactive risk management. 93% of the respondents indicated they are fully aware of cybersecurity practices in their bank while 7% indicated not being aware. The different cybersecurity frameworks adopted by the banking institutions are ISO/IEC 27001 (International Organization for Standardization) leads at 40%, showing it as the preferred international standard. 20% use only internal frameworks, which may lack comprehensive security measures. The distribution across multiple standards (NIST 20%, COBIT 13.3%) indicates a lack of standardization that could create security gaps while 6.7% indicated other standards. A Consultant at Knowledge Network Solutions (KNS College) Freetown remarked: "The lack of standardization is concerning. Banks should align with globally recognized frameworks like NIST (National Institute of Standards and Technology) or ISO to ensure robustness."

On the technical control effectiveness of these frameworks, the analysis reveals that 26.7% rate controls as "very effective" concerning for a high-risk sector. Combined 40.0% view controls as at least "effective", but 20% express doubts. The 13.3% "ineffective" rating reveals potentially vulnerable areas needing attention. In terms of incident preparedness, 66.7% have documented response plans - better than many sectors but still inadequate. 20% lack any plan, creating significant risk exposure. 13.3% uncertainty suggests poor communication about existing plans. An IT specialist at the national commercial bank warned: "Without a clear response plan, banks risk prolonged downtime and reputational damage during breaches."

On the existing gaps in incident response protocols**,** the analysis indicates that most of the respondents are aware of cybersecurity adoption in their institutions. However, there remains a gap where a portion lacks adequate understanding. This highlights the need for widespread awareness programs. Online banking knowledge is relatively high among respondents. This suggests that many have digital engagement with banks, which increases the need for proper digital safety measures. Framework awareness varied, suggesting inconsistent implementation or communication within banking institutions. Banks should prioritise training and visibility of existing cybersecurity. Far while most respondents are aware of cybersecurity, gaps persist. An IT official the national commercial bank noted: "Awareness is the first step, but consistent training is needed to translate knowledge into practice, especially in a sector as dynamic as banking."

- *RQ2: What Challenges Prevent Effective Implementation of Cybersecurity?*

The banking sector in Sierra Leone faces significant cybersecurity challenges that threaten its stability and growth. The most pressing issue identified is the prevalence of outdated systems, which emerged as the top concern from 40 respondents. These legacy infrastructures are particularly vulnerable to modern cyber threats, leaving financial institutions exposed to potential breaches and attacks. Closely following this is the challenge of insufficient funding, cited by 35 respondents. Financial constraints severely limit banks' ability to upgrade their systems and implement robust security measures, creating a persistent vulnerability gap. Compounding these technical and financial challenges is a notable skills shortage, mentioned by 30 respondents, which leaves institutions without the necessary expertise to effectively detect and respond to cyber threats. Governance issues further exacerbate the situation, with weak policies revealed by 25 respondents. This indicates systemic problems in establishing and enforcing adequate cybersecurity protocols across the sector. Together, these challenges form a complex web of vulnerabilities that require immediate and coordinated action.

On cultural attitudes toward cybersecurity affect compliance, in the context of Sierra Leone's banking sector, cultural attitudes significantly influence cybersecurity compliance. Many employees and customers may view security measures such as multi-factor authentication, regular password updates, or restricted data access as inconveniences rather than necessities. This can lead to low adherence to policies, such as sharing passwords or bypassing security protocols for convenience. Resistance to change, especially among staff accustomed to legacy systems or informal workarounds and lack of reporting cybersecurity incidents due to fear of blame or job loss.

- *RQ3: How Can a Context-Specific Cybersecurity Framework Be Designed for Sierra Leone?*

As revealed by a subject expert that the lack of standardization is concerning, banks are advised to align with globally recognized frameworks like NIST (National Institute of Standards and Technology) or ISO to ensure robustness. The Bank of Sierra Leone, the regulatory institution for commercial banks must be stringent in enforcing nest practice global standards. Collaboration between banks and regulators is key to closing compliance gaps.

On the role the Bank of Sierra Leone (BSL) should play in framework enforcement, the findings from the interview revealed, as the central regulatory authority, BSL should play a proactive and enforcement-oriented role in cybersecurity framework adoption. Specifically, BSL should:

- Mandate compliance with internationally recognized frameworks (e.g., NIST, ISO 27001) for all commercial banks;
- Conduct regular audits and impose penalties for non-compliance;
- Provide guidance and support by developing localized cybersecurity guidelines that consider Sierra Leone's infrastructure and resource constraints; and
- Facilitate capacity building through training programs and partnerships with international cybersecurity bodies.

- *RQ4: What are the Methods that Enable Effective Cybersecurity Policy Implementation?*

The findings revealed that cybersecurity is very important to the successful operations of all financial institutions. Cybersecurity is not only considered as being significant to the operations of financial institutions but it also protects them from collateral damage, cyber threats and lack of trust and confidence by their customers. According to the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

findings, highlight a pressing need for enhanced education, stronger communication of security measures, and standardized training protocols. These results underscore the urgency for coordinated action to strengthen cyber resilience across all stakeholder levels, Kraivah (2022).

On capacity building through training programs needed to address staff/customer awareness gaps, the interview discussion revealed that effective training programs should be tailored, continuous, and practical. Additionally, the following were recommended:

- Role-based training for IT staff, frontline employees, and managers;
- Simulated phishing exercises to build practical awareness;
- Customer education campaigns on safe banking practices (e.g., recognizing fraud); and
- Integration of cybersecurity into onboarding and ongoing professional development.

On public-private partnerships in strengthening threat intelligence sharing, the respondents indicated that public-private partnerships (PPPs) can enhance cybersecurity resilience by fostering collaboration between banks, regulators, and government agencies. Specifically:

- Establish a national Cybersecurity Information Sharing Platform where banks can report and receive alerts on emerging threats;
- Regular threat intelligence briefings hosted by BSL or the Ministry of Information and Communication;
- Joint incident response drills involving multiple banks and national cybersecurity agencies; and
- Incentives for participation, such as regulatory recognition or reduced audit frequency for active contributors.

In terms of incentives that would encourage banks to invest in cybersecurity, the respondents opined that banks must be mandated to allocate necessary resources to cybersecurity, a combination of carrots and sticks could be employed:

- Regulatory incentives: Reduced capital requirements or preferential treatment for compliant banks;
- Financial support: Tax breaks, grants, or low-interest loans for cybersecurity upgrades;
- Recognition and certification: Public acknowledgment of banks that achieve cybersecurity milestones; and
- Cyber insurance discounts: Lower premiums for banks with certified security frameworks.

➢ *Customers Awareness in the Adoption of Cybersecurity and its Implications*

Customers are a critical line of defense in a bank's cybersecurity. This section presents their perspective, gauging their awareness of best practices and potential threats. The results help identify key gaps in public knowledge that the banking sector needs to address through education and communication. The study shows that banks and their customers are not on the same page when it comes to safety and communication.

➢ *Critical Knowledge Gap Among Customers*

The most striking finding is the low level of foundational knowledge. A large majority of customers are unfamiliar with essential digital banking concepts: 71.4% of respondent do not know what cybersecurity is. 80% do not know what online banking is. This indicates that a significant portion of the customer base is potentially vulnerable to cyber threats simply due to a lack of basic understanding. They cannot be expected to follow best practices (like creating strong passwords or identifying phishing emails) if they are unaware of the risks.

➢ *Lack of Effective Communication*

The study indicates that bnks are not giving proper orientation to their customers about safety. A large majority 79% of people say their bank has never talked to them about cybersecurity. Due to the banks failure to communicate, almost everyone 97% of customers has no idea what their bank does to protect their money. This is a major communication failure. Banks might have strong security systems, but by not explaining them, they undermine trust and miss a crucial chance to make their customers feel and be more secure.

➢ *Banks are not Teaching their Customers About Safety*

A large majority 79% of people say their bank has never talked to them about cybersecurity. Due to this silence, almost everyone 97% of customers has no idea what their bank does to protect their money. This is a major communication failure. Banks might have strong security systems, but by not explaining them, they undermine trust and miss a crucial chance to make their customers feel and be more secure. This is a huge opportunity. People are not ignoring the problem; they are asking for guidance. If banks start educating their customers, people will be grateful, and everyone will be safer, Marinttious (2023).

IV. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusion

This study concludes that the banking sector in Freetown Western Area Urban faces a multifaceted cybersecurity crisis characterised by a significant gap between policy adoption and effective implementation. Banks are caught between the necessity of digital innovation and the severe constraints of limited resources, outdated infrastructure, and a pronounced skills shortage. While there is a top-level recognition of cyber risks, this has not been met with commensurate investment, standardized training, or a cohesive national regulatory strategy.

The heavy reliance on legacy systems presents a fundamental vulnerability that sophisticated cyber threats can easily exploit. Furthermore, the human element remains the weakest link, with insufficient staff training and a critically low level of customer awareness creating ample opportunities for breaches. The absence of a stringent, enforceable national cybersecurity policy for the banking sector exacerbates these issues, leading to a fragmented and inconsistent security posture across different institutions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

Therefore, without a concerted, multi-stakeholder effort to address these technical, human, and regulatory challenges, the sector remains highly vulnerable to cyber-attacks that could compromise sensitive financial data, disrupt essential services, and undermine national economic stability.

B. Recommendations

Based on the findings and conclusions, the following recommendations are proposed for various stakeholders:

➢ *Bank Management and IT Departments*

A bank's security isn't just built on technology, but on a crucial partnership. Management provides the vision and the resources, asking "What do we need to protect?" The IT team answers with action, figuring out "How do we protect it"? It's this ongoing conversation between the decision-makers and the problem-solvers that truly keeps a bank's doors open and its customers' trust secure. When they work in sync, they don't just defend data; they build a fortress of confidence for everyone who walks through the door. To achieve that they must embark on the following:

- Prioritise Targeted Training: Move from ad-hoc to mandatory, regular, and simulated cybersecurity training for all staff, focusing on phishing, ransomware, and social engineering attacks. Allocate a specific annual budget for continuous human capacity development;
- Phase out Legacy Systems: Develop and fund a strategic, phased plan to modernise core banking systems and IT infrastructure. Prioritise investments in encryption technologies, AI-driven threat detection, and secure authentication methods like Multi-Factor Authentication (MFA);
- Standardise on Frameworks: Fully adopt and implement a recognised international framework like ISO/IEC 27001 or the NIST CSF, rather than relying on internal or multiple standards. They can use this to guide all security controls and incident response planning; and
- Launch Customer Awareness Campaigns: Implement ongoing, multilingual cybersecurity awareness campaigns to educate customers on safe online banking practices, recognising scams, and protecting their credentials.

➢ *Policymakers and Regulators (e.g. Bank of Sierra Leone, NC3)*

Policymakers and regulators, like the Bank of Sierra Leone and the National Cybersecurity Coordination Centre (NC3), act as the architects of a secure financial environment. They set the essential rules and standards that ensure every bank is playing by the same strong rulebook. Their guidance and oversight are crucial for building a unified and resilient defence against cyber threats across the entire banking sector. Policymakers and regulators should embark on the following:

- Enact and Enforce Strong Legislation: Expedite the passage and rigorous enforcement of the Cybersecurity and Cybercrime Act with clear minimum-security standards and penalties for non-compliance for all financial institutions;
- Establish a Centralised Threat Intelligence Platform: Create a national platform for banks to share anonymised threat intelligence and best practices in real-time, fostering a collaborative defence environment;
- Promote Public-Private Partnerships (PPPs): Facilitate partnerships between banks, international organisations, and educational institutions to fund cybersecurity initiatives, sponsor certifications for professionals, and develop local expertise; and
- Incorporate Cybersecurity into Audits: Mandate independent, regular cybersecurity audits as part of the banking license renewal process to ensure continuous compliance and improvement.

➢ *Academic Institutions and Future Research*

Academic institutions are the curious minds asking "what's next?" in cybersecurity. They provide the essential research and cultivate the next generation of Information Technology (IT) talent that the banking sector relies on. By partnering with banks, they help turn theoretical knowledge into real-world solutions, ensuring defences evolve faster than the threats do. Tertiary education institutions must:

- Develop Cybersecurity Curricula: Tertiary educational institutions and Universities should develop specialised undergraduate and postgraduate programs in cybersecurity to build a sustainable pipeline of local talents; and
- Conduct Further Research: Future studies should expand the geographic scope to include rural banks and investigate the specific effectiveness of cost-effective, open-source security tools within the Sierra Leonean context.

In the end, true security is a human endeavour, powered by partnership. It requires management to boldly invest, IT to expertly defend, and regulators to thoughtfully guide. Most importantly, it demands that we bring customers into the fold, transforming them from potential vulnerabilities into informed allies. By weaving these threads together strategy, technology, and trust we don't just protect data; we safeguard the very promise of a secure financial future for Sierra Leone.

REFERENCES

[1]. Al-Alawi, A.I., Al-Bassam, S.A. & Mehrotra, A. (2020). 'The interplay of cybersecurity, regulatory compliance, and business intelligence in the banking sector', Journal of Financial Regulation and Compliance, 28(4), pp. 567-583.
[2]. Bank of Sierra Leone (2023). Annual Report and Statement of Accounts 2022. Freetown: Bank of Sierra Leone.
[3]. British Bankers Association (BBA) & PricewaterhouseCoopers (PwC) (2014) Cyber and the City: Managing Cyber Risk in the Financial Sector. London: PwC.
[4]. Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches. 4th ed. Thousand Oaks, CA: Sage Publications
[5]. Cryer, S. & Zounlome, N. (2018). 'The effectiveness of simulated phishing attacks in improving employee cybersecurity behaviour', Journal of Information Security, 9(3), pp. 215-228.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb405

[6]. Dawodu, A., Johnson, J. & Ogunlana, A. (2023). 'A systematic review of cybersecurity frameworks for the financial services industry', Computers & Security, 124, 102956.
[7]. Desai, P. & Hamid, S. (2021). 'Cloud security challenges in the financial sector: A review of compliance and technical issues', International Journal of Cloud Applications and Computing, 11(2), pp. 45-62
[8]. Girling, P. (2022). Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework. Hoboken, NJ: Wiley.
[9]. ISMS_online (2025). What is ISO 27001? Available at: https://www.isms.online/iso-27001/ (Accessed: 15 July 2025).
[10]. Jain, A., Singh, R. & Kumar, P. (2023) 'The evolution of cybercrime in the era of fintech and digital banking',Journal of Financial Crime, 30(1), pp. 145-160.
[11]. Kamara, M. (2019) Digital Banking and Financial Inclusion in Sierra Leone. Freetown: Sierra Leone Publishing
[12]. Kamara, M. (2023) 'Building cybersecurity capacity in Sierra Leone: The role of the National Cybersecurity Coordination Centre (NC3)', West African Journal of Information and Communication, 12(1), pp. 45-60.
[13]. Kawimbe, C. & Kwalombota, D. (2024) 'Cybersecurity implementation challenges in the Zambian banking sector: A mixed-methods study', African Journal of Information Systems, 16(2), pp. 78-95.
[14]. Kuepper, J. (2017) 'The rising tide of cybercrime in global banking', The Economist Intelligence Unit. Available at: https://www.eiu.com/ (Accessed: 10 June 2025).
[15]. Marican, Y., Abdullah, L. & Hussin, M. (2022) 'Cybersecurity maturity in fintech startups: A critical review', Journal of Cybersecurity Technology, 6(3), pp. 189-205.
[16]. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1979) The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Washington, D.C.: U.S. Department of Health & Human Services.
[17]. Obi, C., Usman, A. & Shobowale, S. (2024) 'The role of employee training in mitigating insider threats in the banking sector', Security Journal, 37(1), pp. 112-130.
[18]. Saeed, S., Altamimi, S. & Asif, M. (2023) 'Adoption of cybersecurity frameworks in developing economies: A case of the Middle East and Africa', Information & Computer Security, 31(2), pp. 234-251.
[19]. Sawaneh, I. (2018). “An Assessment of Cyber Security Threats in Sierra Leone”. Freetown: IPAM – USL (unpublished dissertation).
[20]. Sawaneh, I. (2024), 'Cultural and structural barriers to cybersecurity compliance in West African banks', Journal of African Business, 25(1), pp. 88-105.
[21]. Sulistyowati, D., Hidayat, B. & Prasetyo, A. (2023) 'Implementing ISO 27001 for data protection in banking: Lessons from Southeast Asia', International Journal of Information Management, 68, 102572.
[22]. Summerfield, M. (2014). “The Impact of Digital Technology on Banking”. New York: Palgrave Macmillan.