Overview of the CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks

G. ELIAS

Introduction

On May 31, 2024, the Central Bank of Nigeria ("**CBN**") issued the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks (the "**Framework**"). The Framework provides the minimum requirements that deposit money banks ("**DMBs**") and payment service banks ("**PSBs**") must put in place in their respective cybersecurity programmes. The Framework applies to DMBs and PSBs, including commercial banks, merchant banks and non-interest banks, referred to together as supervised financial institutions ("**SFIs**"). SFIs are required to comply with the provisions of the Framework from the effective date of July 1, 2024. The Framework was issued to guide the implementation of cybersecurity programmes to enhance resilience in the financial sector. This article (a) compares the Framework with the previous cybersecurity regulatory regime for SFIs and (b) examines the provisions of the Framework. The main changes introduced by the Framework include having better balanced blends of directors and setting out in great detail the risk management features that DMBs and PSBs must implement. The Framework is written clearly, and its issuance and content are welcome.

Some Broad Changes

The previous cybersecurity regulatory regime for SFIs was the "Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018" (the "**Previous Framework**"). The Previous Framework was divided into five parts and did not provide for of emerging technologies. While the Previous Framework recognized the board of directors (the "**Board**") of SFIs as having the overall responsibility of cybersecurity governance, it did not mandate the requirement that certain members of the Board must be skilled in information communication technology ("**ICT**") and cybersecurity knowledge.[1]

The Framework requires at least two (2) non-executive directors ("**NEDs**") of the Board of an SFI, of whom one (1) must be an independent NED, to have requisite knowledge and experience in innovative financial technology, ICT and/or cybersecurity.[2]. The risk management system of the Previous Framework did not cover the risk identification process now provided in the Framework. While the Framework provides for third-party risk management for mitigating cybersecurity risks associated with third parties, the Previous Framework did not contain such provisions.[3]

Scope of the Framework

The Framework is divided into seven (7) parts which include: (a) cybersecurity governance and oversight; (b) cybersecurity risk management system; (c) enhancing cybersecurity resilience; (d) emerging technologies; (e) metrics, monitoring and reporting; (f) compliance with statutory and regulatory requirements; and (g) enforcement. Below, we look clearly at each of these seven areas.

1. Cybersecurity Governance and Oversight

The Framework provides that the Board, through a Board Risk or Information Technology Committee, has the oversight and responsibility for the cybersecurity framework of an SFI. The Board of an SFI is required to provide the leadership, direction and resources to effectively conduct the required processes and ensure the integration of cybersecurity governance into the SFI's organisational structure.[4] The Framework sets the minimum number of NEDs and the requirement for an Independent NED to have requisite experience in financial technology, ICT and/or cybersecurity.

[1] Para. 2 of the Previous Framework.
[2] Para. 1.1(i) of the Framework.
[3] Para. 2.9 of the Previous Framework.
[4] Para. 1.1 of the Framework.

The Board is responsible for preparing quarterly reports detailing the overall status of the cybersecurity programme of an SFI and such reports must include at a minimum: (a) a cyber risk assessment report or updates from the last assessment; (b) the status of security initiatives to address cyber risks; (c) the number of incidents recorded, status of losses and recoveries; and (d) vulnerability management/penetration test reports, remediation efforts and challenges encountered and compensating controls implemented.[5]

2. Cybersecurity Risk Management System

SFIs are required to carry out the following activities under the risk management system:

2.1. **Risk Identification**: SFIs are required to identify threats and vulnerabilities associated with the confidentiality, integrity and availability of their information assets to determine their cyber risk exposure.[6]

2.2. **Risk Assessment**: SFIs must evaluate the risk to their operations and consider the probability of occurrence of such risks. The risk assessment process must be conducted annually and whenever major changes (such as an acquisition, merger or deployment of new technology) occur within an SFI. The outcome of every risk assessment process must be documented by an SFI in a cybersecurity risk control self-assessment.[7] SFIs, are to submit to the CBN, the cybersecurity self-assessment in a format prescribed by the CBN from time to time annually, no later than February 28.

2.3. **Risk Measurement**: SFIs are required to quantify the financial impact of cybersecurity risks through the risk measurement process.[8]

2.4. **Risk Mitigation/Treatment**: SFIs are required to implement risk mitigation and control measures consistent with the criticality of information assets. Risk treatment options such as risk reduction, acceptance, avoidance, transfer and management of residual risk should be selected based on the outcome of the risk assessment.[9]

2.5. **Risk Monitoring and Reporting**: An independent risk management function is to be established and become responsible for assessing, measuring, monitoring and reporting the risks associated with IT infrastructure and services. SFIs must also maintain a risk register to facilitate the monitoring and reporting of risks.[10]

2.6. **Third Parties**: In addition, the Framework provides that SFIs must employ third-party risk managers to assess and mitigate the risks associated with third-party relationships. These include the SFI's vendor selection process, due diligence, contract negotiations, ongoing monitoring and incident response. SFIs must perform at least an annual cybersecurity awareness programme to inform stakeholders. Service level agreements should also clearly specify the SFI's right to audit third parties or receive audit reports. The Framework mandates third-party service providers to comply with relevant regulatory standards based on the services offered (*e.g*. PCIDSS, NDPR, ISO27001, ISO 8385).

3. Enhancing Cybersecurity Resilience

The Framework provides that SFIs must establish procedures to enhance cyber resilience, which is the ability to prevent, withstand and recover from cyber incidents. SFIs must ensure that the

[5] Para. 1.1(viii) of the Framework.
[6] Para. 2.1.1 of the Framework.
[7] Para. 2.1.2 of the Framework.
[8] Para. 2.1.3 of the Framework.
[9] Para. 2.1.4 of the Framework.
[10] Para. 2.1.5 of the Framework.

following minimum controls are put in place: (a) know your environment measures which include familiarizing with its business environment and identifying critical assets; (b) implement preventive controls; (c) establish the capacity for monitoring and detecting cyber anomalies or incidents; (d) ensure that capacity for responding to cyber incidents are available in-house or can be outsourced at short notice; and (e) participate in industry-specific cyber exercises and programmes to evaluate its level of preparedness to recover from cyber incidents.[11]

4. Emerging Technologies

The Framework recognizes innovations in the early stages of development and adoption that SFIs currently employ in banking operations and to improve customer experience. Some of the emerging technologies recognized include: (a) payment methods including (i) contactless payments, quick response codes, (ii) voice-initiated services, (iii) unstructured supplementary service data (USSD) codes; (b) open banking; (c) distributed ledger technology; (d) artificial intelligence and machine learning; and (e) the internet of things.[12] SFIs are required to obtain the CBN's approval before deploying emerging technologies and products and ensure that the products are not offered by countries on the sanctions list.[13]

5. Metrics, Monitoring and Reporting

SFIs must review metrics such as key performance indicators, key risk indicators, key goal indicators at least annually. Incidences of cyber incidents should be reported to the CBN within twenty-four (24) hours after such incidents occur.[14]

6. Compliance with Statutory and Regulatory Requirements

The Board and senior management of SFIs must comply with applicable statutes and regulations to avoid breaching legal, statutory and regulatory requirements on cybersecurity.[15] Non-compliance with the Framework will attract appropriate sanctions provided in the Banks and Other Financial Institutions Act, 2020 and other regulations.[16]

7. Enforcement

CBN will monitor and enforce compliance with the provisions of the Framework and carry out monitoring and enforcement through annual cybersecurity supervisory review and evaluation exercises, risk-based examinations, annual industry compliance audits and periodic spot checks.[17]

Conclusion

Given the increase in security threats and the prevalence of emerging technologies in the financial system, the issuance of the Framework by the CBN is a welcome development. It is expected that the additional obligations imposed on SFIs by the Framework would enhance public confidence and mitigate risk factors in the financial system. It is expedient that SFIs comply with the cybersecurity measures and obligations imposed by the Framework to reduce and mitigate cybersecurity risks and attacks that are continually on the rise. In any event, SFIs face the risk of regulatory sanctions when they fail to comply with the Framework from its effective date, being July 1, 2024.

[11] Para. 3 of the Framework.
[12] Para. 4 of the Framework.
[13] Para. 4.8 of the Framework.
[14] Para. 5 of the Framework.
[15] Para. 6 of the Framework.
[16] Para. 6(iii) of the Framework.
[17] Para. 7 of the Framework.

Authors

Larry Nkwor
Associate
larry.nkwor@gelias.com

Larry Nkwor is an associate in the firm's dispute resolution and new economy practice groups. He advises local and international clients on corporate transactions, finance and compliance and represents clients in high profile disputes. His major practices cover litigation, arbitration, technology law, fintech, data privacy, telecommunications and entertainment law.

Iyanuoluwa Adeyemo
Associate
iyanuoluwa.adeyemo @gelias.com

Iyanuoluwa Adeyemo is an associate in the firm's Energy, Banking and Finance and New Economy practice groups. Her major practices cover oil and gas, project finance, banking, fintech, litigation and infrastructure development.

LOCATIONS

LAGOS OFFICE
6 Broad Street
Lagos, Nigeria

T: +234 (1) 460 7890
E: gelias@gelias.com

ABUJA OFFICE
2nd Floor, Abia House,
Plot 979, First Avenue,
Central Business District
F.C.T, Abuja.

T: +234 (1) 888 8881

Practices ● Arbitration ● Banking ● Capital Markets ● Competition ● Compliance ● Corporate ● Data Protection ● Derivatives ● Employment ● Fintech ● Foreign Investment ● Intellectual Property ● Litigation ● Mergers and Acquisitions ● Tax ● "White Collar" Sanctions ●

Sectors ● Agribusiness ● Commercial Banks ● Commodities ● Construction ● Distributors ● Development Finance ● Electric Power ● Entertainment ● External Trade ● Fintech ● Healthcare ● Infrastructure ● Insurance ● Investment Banks ● Manufacturing ● Media ● Mining ● Oil and Gas ● Pension Managers ● Private Equity ● Real Estate ● Services ● Technology ● Telecommunications ● Transport ●

www.gelias.com