**23AC1 CYB6012- Cyber Project 1**

Project Title: Cyber Resilience Assessment of an OFI

**Background:**

The Central Bank of Nigeria (CBN) is the regulatory institution for Other Financial Institution in Nigeria. The 1958 CBN Act of Parliament, as amended in 1991, 1993,1997,1998,1999 and 2007 establishes the CBN and its regulatory powers over certain institutions.

As part of its oversight functions, the CBN recently issued the Risk Based Cybersecurity Framework and Guidelines to OFIs (‘the guidelines’) outlining the minimum requirements they are to observe in developing and implementing strategies, policies, procedures and related activities aimed at mitigating the risks of cyberthreats and attacks.

This started in form of an Exposure Draft circulated to the OFI’s for comments in August 2021 following which the framework and guidelines were issued on 29th June 2022. Microfinance Banks (MFB) are considered as part of Other Financial Institutions (OFI) by regulators in Nigeria. Hence, compliance with the Risk Based Cybersecurity Framework and Guidelines is expected.

Seoul Microfinance Bank[[1]](#footnote-1) (SMFB) is a Lagos based financial institution that has been in operation for more than three decades and plans to continue in profitable business for the years to come. As a Unit MFB, its operations are relatively small but very important to the financial inclusion of those in the lower rung of the society through the taking of deposits and the provision of short-term loans.

**Justification:**

This project will assist SMFB, classified as an OFI by the CBN, to comply with the provisions of the Risk Based Cybersecurity Framework and Guidelines.

Compliance with CBN guidelines is a condition upon which the approved license to operate as an OFI is based and while no sanctions are stated in the guideline for non-compliance, the External Auditor of the bank is expected to report instances of non-compliance with guidelines to the users of the Financial Statement and the CBN with the probable result that continued non-compliance may lead to heavy sanctions and the withdrawal of the license to operate.

OFI’s are expected to comply with effect from 1st January 2023 but the majority of OFIs (including SMFB) are challenged both from a knowledge-gap and financial capacity to meet the responsibilities detailed in the guideline, hence non-compliance is currently widespread.

There are current discussions between the MFBs and their umbrella body The National Association of Microfinance Banks (NAMB) on approaching the CBN on a host of concerns regarding compliance with the guidelines such as the effective date as well as the expected level of compliance.

**Scope (in and out of scope)**

The guidelines are divided into six parts:

* cybersecurity governance and oversight.
* cybersecurity risk management system.
* cyber resilience assessment.
* cybersecurity operational resilience.
* cyberthreat intelligence and metrics.
* monitoring; and
* reporting.

Of these, what is in scope will be the cybersecurity operational resilience. The guidelines require OFIs to build, enhance and maintain their cybersecurity operation resilience by putting in place minimum controls, such as know-your-environment and other operational resilience measures or controls to the confidentiality, integrity and availability of information assets, among other things.

**In Scope Activities:**

The scope of this project is limited to the assessment of the entity’s information system, the controls currently in place as well as the infrastructure that supports the confidentiality, integrity and availability of the same to enhance the business of the entity.

Consequently, the following activities are in scope of this project:

1. inventory the Information Technology assets and enabling infrastructure to understand the hardware, software, firmware, and systems within the entity.
2. conduct the cybersecurity self-assessment be to determine both its present state and its target or desired cybersecurity profile or state.
3. Graphical user interface, diagram, schematic

   Description automatically generatedidentify gaps, threats, and risks.
4. identify the potential impact.
5. prioritize action plans to mitigate the risks identified.
6. provide a timeline for remediation; and
7. provide a remediation status with possible residual vulnerabilities and risks.

**Out of Scope Activities:**

The following activities are out of scope of this project:

1. Implementation of Recommendation
2. Maintaining the Assessment
3. Follow-Up Audit on Implementation

Figure 1: Extracted from NIST 800-30

1. Communication with the CBN

**Methodology,**

The United States Department of Commerce’ National Institute of Standards and Technology has issued a Guide for Conducting Risk Assessments which is widely accepted as a standard across the world, including Nigeria. The Resilience Assessment of SMFB’s will follow the processes established by this guide.

Figure 2: The Risk Assessment Process – NIST Special Publication 800-30

Using the Risk Assessment process will be composed of the following steps:

1. prepare for the assessment.
2. conduct the assessment.
3. communicate assessment results; and
4. maintain the assessment.

In terms of maintaining the assessment, the project will be limited to only recommending steps for maintenance and would not be involved in actually maintaining the assessment.

**Potential blockers and mitigation strategies,**

1. The effective date for the guideline being 1st Jan 2023 and a reporting requirement by 31st March 2023. These deadlines have been discussed with SMFB and there are no current alternative plans to meet the dates. SMFB is in discussion with NAMB and a few other OFI’s to seek a waiver from meeting these dates.
2. Physical access to Equipment and Infrastructure – While the majority of the work can be done remotely using Digital Forensic Tools, there may be some infrastructure that will require physical access. The IT Administrator will be used to cover such scope and if necessary, a trip to Nigeria will be planned
3. Penetration Testing Tools – For the purposes of this project, resulting from budget constraints, heavy reliance will be placed on the use of freely available penetration testing tools and exclude use of commercial and paid software and tools. The mitigation for this constraint is to include a ‘caveat’ in the report drawing attention to the continued existence of risks of compromise resulting from adversaries use of sophisticated tools which are out of scope of the project.

**Project output**

The plan is to produce a report on the cybersecurity self-assessment detailing the vulnerabilities in the existing system and a mitigation plan that addresses these as well as emerging threats.

**Ethical concerns,**

1. Harms to privacy – This project will receive and evaluate sensitive operation data of the entity being assessed. In addition, being an operating financial institution, the project may come across sensitive personal information relating to its clients and stakeholders. If these information were to get in the hands of adversaries and threat actors, this may result in costly spam, phishing, or other undesirable communications.

The following steps have been agreed to address these:

* 1. The recipients of the information have agreed to only use these information for the purpose of educational evaluation alone and have further agreed to:
     1. Protect these information from being accessed by third-parties
     2. Destroy these information following the expiration of the reasonable use period
  2. Correspondence including information relating to the entity will only be communicated using encrypted email service

1. Transparency and disclosure – The entity has been informed about the ‘use’ case for this project and has agreed to support the project and give permission only for data collected and report outcomes to be disclosed and used for educational assessment purpose within limited time.

**Stakeholders:**

1. The Regulatory Authority – When completed, it is reasonably expected that the project report may be considered as a key input for the entity’s submission to the regulatory authority, the CBN, to demonstrate compliance with the guidelines
2. The Board of Directors – The board of directors have responsibilities under the guidelines and the reports from this project may be submitted to the board by Management and its recommendation may be used in policy development within the entity
3. Service Providers – especially business enhancing IT service providers whose processes and services may be impacted from the findings and recommendations deriving from the project.
4. Edith Cowan University (ECU) – The Unit Coordinator & Facilitator for the Capstone Cyber Project 1 CYB6012 (23AC1) will provide guidance, supervision and assessment of the project

**Suitability for the project**

I grew up in Nigeria before migrating to Australia and have extensive work experience and network acquired in the country. In addition, I had worked in the financial sector for years with a great understanding of the operations of the money market in Nigeria.

Regarding SMFB, I have significant influence over its operations derived from being a stakeholder. When the Exposure Draft was issued initially in August 2021, I was requested by SMFB to assist to provide some feedback to the CBN, which I did.

**Project schedule in Gant Chart**.

This will be developed and submitted later on.

1. This is a fictitious name chosen in order to anonymize the real entity that is the subject of the project. This is important in order not to compromise the entity’s cyber security through intentional and unintentional disclosure of the existing processes, infrastructure and their vulnerabilities which could be used by adversaries negatively. [↑](#footnote-ref-1)