

|  |  |
| --- | --- |
| CYB6012 (Cyber PROJECT 1) – project proposal | |
| **Study Period:** | 23AC1 |
| **Student:** | Oluwaseun Abimibola BAKARE |
| **project title:** | Cyber Resilience Assessment of an OTher FINANCIAL INSTITUTION |
| **Facilitator:** | Bazlur Rashid |
|  | |

**Executive Summary**

The Cyber Resilience Assessment of Seoul Microfinance Bank[[1]](#footnote-1) (SMFB) will assist the bank with complying with the cybersecurity operational resilience aspect of the Central Bank of Nigeria (2022) Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions.

SMFB aims at delivering superior returns to its shareholders. A cyber incidence will hinder SMFB from achieving its goal. This is because a cyber incidence is costly – it has costs relating to dealing with reputational damage and regulatory monitoring issues. More so, it takes resources away from other more productive uses.

This project, in addition to meeting a compliance obligation, also helps to reduce the risk of a cyber incidence by decreasing the threat landscape available to adversaries. It achieves this by auditing the current cybersecurity posture of the bank and providing actionable advice that, when implemented, will strengthen existing systems, and defend in-depth the bank’s information systems. In so doing, the Confidentiality, Integrity, and Availability of the information that provides the bank a competing edge in the market is enhanced

The following are some additional value-drivers for the project:

1. Reduction of long-term costs,
2. Avoidance of sanctions and penalties that may arise from regulatory non-compliance issues.
3. Avoidance of loss of revenue from business downtime.

At the end of the current phase of the project, the prepare phase, stakeholders were identified, engaged and alignment obtained on the project’s scope of work, resources, cost estimate and schedule for completing the project. Also, the project’s risk matrix was developed alongside a data breach plan which was informed by considerations regarding data privacy issues.

On completion, the project will provide stakeholders with a Cybersecurity Vulnerabilities and Threats Assessment Report of the bank along with suggested counter measures to take to mitigate these. The Cybersecurity Risk Assessment Template used by the project would also become available for the bank to use for future assessments.

**Objectives of the project**

To accomplish the above aim, the project will:

1. Evaluate the vulnerabilities in the system. Use the frame work developed by Singh et al. (2016) to estimate the risk level through the combined use of information available on the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS).
2. Based on the bank’s threshold of acceptable risks, in the light of threats in the Nigerian financial sector, create a Financial Impact Assessment Scale (Driz, 2017)that shows the magnitude of impact if any of the vulnerabilities identified in (a) above is exploited.
3. Using the Financial Impact Assessment Scale along with a Probability Scale, determine the Threat Severity Level and
4. Develop recommendations to close gaps discovered and prioritize these, based on the Threat Severity Level in (c) above.

When completed, this project would help SMFB to achieve the following:

1. Reduce Long-Term Costs, saving the bank from reputational damage that may arise from a cyber incident. According to Rinaldi (2023), a cyber incident may cost a small business between $120,000 to $1.24m.
2. Increase awareness of Cybersecurity within the bank so as to help in combating social engineering attacks. Goh (2021)informs that humans are the weakest player in the maintenance of cybersecurity. This position is reinforced by The Human Factor 2022 report (Proofpoint, 2021)showing that workers continue to take cyber risks and threat actors are capitalizing on this, getting better at employing social engineering in their attacks.
3. Compliance with the Central Bank of Nigeria (CBN) guidelines and avoid sanctions and penalties that may arise from regulatory non-compliance issues.
4. Avoid Loss of Revenue from business downtime
5. Provides a Cybersecurity Risk Assessment Template that the bank may use for future assessments.

**Justification**

The 1958 Central Bank of Nigeria Act of Parliament, as amended, established the CBN and assigned it regulatory powers over certain institutions amongst which are the Other Financial Institutions (OFI).

The Central Bank of Nigeria is the apex financial institution with the overall control and administration of the monetary policies of the Federal Government of Nigeria. One of its aim is to “promote a sound financial system in Nigeria” and it accomplishes this by administering the Banks and Other Financial Institutions Act (BOFIA), 2020 (Central Bank of Nigeria, n.d)

Compliance with CBN guidelines is a condition upon which the approved license to operate as an OFI is based and, by law, 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 (Central Bank of Nigeria, 2012) with the expectation that continued non-compliance may lead to heavy sanctions and the withdrawal of the license to operate.

Seoul Microfinance Bank (SMFB) is a Lagos based OFI that has been in operation for more than three. Its operations are relatively small but very important to the financial inclusion of those in the lower strata of the society through the taking of deposits and the provision of short-term loans.

Microfinance Banks (MFB) are considered as part of OFIs by regulators in Nigeria. Hence, compliance with the Risk Based Cybersecurity Framework and Guidelines is expected with effect from 1st January 2023. Arising from knowledge-gap and financial incapacity to meet the responsibilities detailed in the guideline, non-compliance is currently widespread amongst OFIs (including SMFB).

According to Perols and Murthy (2021), cybersecurity incidents result in erosion in investment in the enterprise arising from negative investors’ perceptions of audit quality. It becomes imperative to carry out this project as it helps steer the bank towards accomplishing its vision of maximizing investors wealth.

Arising from my education in Cybersecurity and long-time association with SMFB, I am in good stead to assist the bank in addressing this non-compliance challenge.

**Scope**

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:**

Though the guidelines are divided into six parts, what is in scope will be the cybersecurity operational resilience element. To achieve this, the following activities are in scope of this project:

1. Graphical user interface, diagram, schematic

   Description automatically generatedinventory the Information Technology assets, network and enabling infrastructure.
2. conduct the cybersecurity assessment be to determine both its present state and its target or desired cybersecurity profile or state.
3. identify gaps, threats, and risks.
4. identify the potential impact.
5. prioritize action plans to mitigate the risks identified, noting that in line with Whitman and Mattford (2017) five (5) Information Security Risk Control Strategies not all risks can be defended.

Figure 1: The Risk Assessment Process – NIST Special Publication 800-30

1. suggest a tracking methodology to assure that actions are implemented and closed.

**Out of Scope Activities:**

The following activities are out of scope of this project:

1. Implementation of Recommendation

Management is responsible for the day-to-day running of the bank and deciding on what recommendations to implement and when, is a management responsibility. Consequently, this is out of scope for this project.

1. Follow-Up Audit on Implementation

Edwards-Faulk and O'regan (2012)posit that an integral part of an auditor’s responsibility is to follow up on the implementation status of audits. However, arising from limited resources and the fact that this is an academic exercise, following up on the implementation status of recommendation is out of scope for this project.

1. Communication with the CBN

The responsibility to report the outcome of this project to the CBN will remain that of Management. Neither this project findings or work files will be made available to the CBN.

**Proposed 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.

Using the Risk Assessment process as suggested in the guideline include 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 maintaining the assessment.

**Risks**

An initial project risk assessment has been carried out and the following are the identified risks along with their likeliness of occurrence and impact. As part of the project’s risk management plan, these risks and emerging ones will be continually monitored, updated and strategies to mitigate them developed as the project goes through execution.

**Risk Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Negligible | Minor | Moderate | Major | Catastrophic |
| Very Likely |  |  | Current Fuel and Money Supply crises |  |  |
| Likely |  | Adequate IT and Cybersecurity skills | Adequate tools to conduct the needed tests | General Staff buy-in to support the project |  |
| Possible |  | Documentation of existing system | The Nigerian Election and its aftermath | Network Access |  |
| Unlikely |  |  |  |  |  |
| Very Unlikely |  |  |  |  |  |

**Resources**

In terms of human resources, the project team consists of one Analyst aided by the IT staff available within SMFB. The other resources to be used are:

Table

Description automatically generated

Figure 2: Listing of Project Resources

**Project schedule**

A project schedule has been developed using the MS Project Professional. The major milestones in the project are as extracted and shown in the chart below. The detailed Project Gantt Chart is attached as an appendix.

Diagram, schematic

Description automatically generated

Figure 3: Project Schedule Summary

**Legal, ethical, or social considerations**

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 threat actors, this may result in costly spam, phishing, or other undesirable communications.

The following steps have been agreed to address these:

1. All works relating to the project will be carried out on a whole-disk encrypted laptop to prevent unauthorized access to the project data.
2. Remote connection to the bank’s network shall be through AnyDesk, a cryptography Virtual Private Network (VPN).
3. No USB drives will be used for the project.
4. All reports and documents generated will be sent to the bank’s Director using the Advanced Encryption Standard (AES).
5. ECU recipients of the information have agreed to only use these information for the purpose of educational evaluation alone and have further agree to:
   1. Protect these information from being accessed by third parties.
   2. Destroy these information following the expiration of the reasonable use period.
6. All data collected will be ethically destroyed following the completion of the project work.
7. 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.
8. Compliance with all Applicable Laws - The Analyst will abide with the Australian Information Security Association (2018) Code of Ethics and Conference Behaviour Rules.
9. Non-disclosure Agreement - all non-public information obtained from this project is confidential information. Confidential Information would not be disclosed to third parties without prior written consent of the bank.

**References**

Australian Information Security Association. (2018). *Code of Ethics and Conference Behaviour Rules*. Retrieved 13/09/2022 from <https://www.aisa.org.au/common/Uploaded%20files/aisa_code_of_ethics_-_final_v2.pdf>

Central Bank of Nigeria. (2012). *Revised Regulatory and Supervisory Guidelines for Microfinance Banks in Nigeria*. Retrieved from <https://bit.ly/3xf8vgJ>

Central Bank of Nigeria. (2022). *Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions*. Retrieved from <https://bit.ly/40ImCsB>

Central Bank of Nigeria. (n.d). *About CBN*. Retrieved 24/02/2023 from <https://www.cbn.gov.ng/AboutCBN/>

Driz, S. E. (2017). 7 Steps to Prioritize Cyber Security Threats & Threat Remediation. <https://bit.ly/3DZIHsK>

Edwards-Faulk, P., & O'regan, D. (2012). The importance of following up: audits don't end after the report has been issued--in fact, risks may arise if practitioners fail to perform post-audit checks. *Internal Auditor*, *69*(6), 19-22.

Goh, P. (2021). Humans as the weakest link in maintaining cybersecurity: Building cyber resilience in humans. In *Introduction To Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators* (pp. 287-305).

Perols, R. R., & Murthy, U. S. (2021). The impact of cybersecurity risk management examinations and cybersecurity incidents on investor perceptions and decisions. *Auditing: A Journal of Practice & Theory*, *40*(1), 73-89.

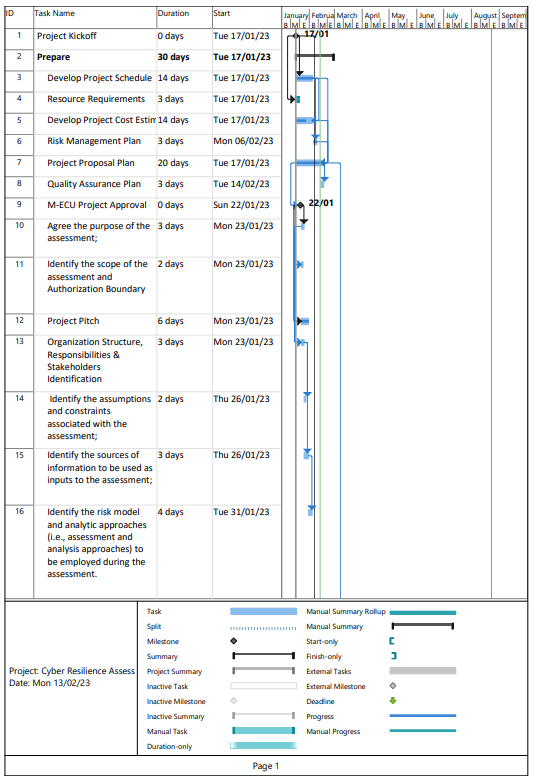
Proofpoint. (2021). *The Human Factor 2022* (Threat Report, Issue. <https://www.proofpoint.com/au/human-factor#mktoForm_3414>

Rinaldi, A. (2023). The Cost of Cybersecurity and How to Budget for It. Retrieved 08/02/2023, from <https://www.business.com/articles/smb-budget-for-cybersecurity/>

Singh, U. K., Joshi, C., & Gaud, N. (2016). Information security assessment by quantifying risk level of network vulnerabilities. *International Journal of Computer Applications*, *156*(2), 37-44.

Whitman, M. E., & Mattford, H. (2017). *Management of information security* (Fifth edition. ed.). Cengage.

APPENDIX



Graphical user interface

Description automatically generated with medium confidence

A picture containing graphical user interface

Description automatically generated

1. This is a random name that is chosen and used to anonymize the real Microfinance Bank that is the subject of the project. This is an important part of the ethical consideration to ensure the privacy of the data that will be used in this project. [↑](#footnote-ref-1)