Scope Draft

To achieve the dual aim of the project – compliance with regulations and aiding Seoul Microfinance Bank (SMFB) to meet its vision, the following represent the scope of work that will be undertaken by the project.

## 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. inventory 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.
6. 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.