Nist CSF 1.1 assessment report for ‘Alfa Bank Institute’, a bank operating in 2 different Countries.

1. Asset Management (ID.AM):

Alfa Bank Institute does not appear to have a clear understanding of the critical resources and sensitive data that must be protected, such as all the IT assets used by people who process mortgage loans or provide consultancy by accessing specific bank account data.

Failure to identify critical assets could lead to inadequate protection of sensitive data, increasing the risk of data breaches and compromises (all devices used to access information must be censored and audited).

Identifying and categorizing critical assets helps focus security measures and ensure adequate protection of sensitive information. The Information Technology function is therefore asked to survey the IT assets in the light of the classification rules provided by the internal Compliance & Information Security function, in order to comply in particular with the following controls:

- ID.AM-1: The identification and inventory of physical devices and systems in particular used for financial management (such as database servers and payment systems) within the organization allows them to be monitored and adequately protected. This reduces the risk of unauthorized or unmanaged devices being used to access sensitive data or compromising security, and malicious actors being able to access or manipulate those resources for fraudulent purposes.

- ID.AM-6: The implementation of a risk-based data classification allows the organization to apply appropriate security measures to each category of data. This ensures that sensitive data is protected according to the banking institution's regulatory needs and risk tolerance.

2. Access Control (ID.AC):

Alfa Bank Institute does not have a clear policy to define the flows of activation and de-provisioning of utilities (provisioning and de-provisioning).

Excessive or inappropriate access privileges can lead to internal abuse or unauthorized access, putting data confidentiality and integrity at risk. Some people turned out to have incompatible or unnecessary profiles with respect to the tasks performed, having not been able to justify their use with respect to the tasks.

In particular, the Compliance & Information Security function is asked to provide a more detailed policy on user activation flows and stronger rules on password policies in line with the following controls:

- ID.AC-2: Assigning users the appropriate access rights based on their role and responsibilities reduces the risk of unauthorized access or internal abuse. This ensures that only authorized persons have access to sensitive assets (especially financial ones) and limits the possibility of data manipulation or theft.

- ID.AC-5: Periodically changing authenticators, such as passwords, reduces the risk of unauthorized access due to compromised or stolen passwords. Frequently updating authenticators limits the effectiveness of attacks based on previously obtained passwords.

3. Awareness and Training (ID.AT):

Alfa Bank Institute does not have adequate safety awareness and training programs for personnel with respect to the specific risk. Lack of security awareness among employees can increase the likelihood of incidents caused by human error or social engineering attacks, and an effective security training program ensures that personnel are aware of security best practices, thereby reducing the risk of accidents caused by human errors or attacks. Specifically, Human Resources and the Compliance & Information Security function are required to schedule and deliver information security training to meet the following requirements:

- ID.AT-1: Providing a security training program to all employees educates staff about security risks and good cybersecurity practice, helping to raise awareness about protecting financial information and common fraud methods. This reduces human errors, such as opening suspicious attachments or clicking on malicious links, which could lead to security breaches, ie it reduces the possibility of employees falling victim to fraudulent activity.

- ID.AT-4: Communicating security information to external stakeholders, such as customers, enables them to take appropriate security measures. This awareness reduces the risk of social engineering attacks, where external users can be tricked into acting insecurely or disclosing sensitive information.

4.Data Security (ID.DS):

Alfa Bank Institute does not correctly survey and regulate the encryption methods used for the processing of information in transit and at rest. In some cases, when storing sensitive data relating to banking relationships, the data is stored without any form of encryption. With reference to the transfer of internal data from one site to another, these take place with an insecure ftp protocol. In particular, the Information Technology, Compliance & Information Security functions, with the budget guaranteed by the Board of Directors, should work together to implement in particular the following controls:

- ID.DS-2: Securing data in transit through the use of encryption technologies reduces the risk of unauthorized interception of financial data. This ensures that sensitive data transmitted via external networks or channels is encrypted and protected against unauthorized reading or manipulation, ie, in particular, that customers' financial information is protected from unauthorized access and that financial transactions are secure.

- ID.DS-5: Verifying data integrity using cryptographic checksums reduces the risk of data corruption. This ensures that the data has not been altered or compromised during its storage or transmission.

5. Incident Response (ID.IR):

Alfa Bank Institute has an incident management procedure for all the areas required by the applicable legislation in the country in which it operates (mandatory for banking institutions), but it is not very accurate with respect to the management of security events that concern internal processes extraneous to banking operations, but capable of having an impact on the institution's operations. In particular, the Compliance & Information Technology function will have to analyze the possibilities for improving the current procedures in order to reach a more appropriate level of maturity of the implementation, in line with the following controls:

- ID.IR-1: Developing, implementing and testing an incident response plan enables the bank to respond in a timely, effective and repeatable manner to any security breach. This limits the potential damage caused by an accident and helps restore safety as quickly as possible.

- ID.IR-4: Communication and coordination with external stakeholders during security incidents, such as law enforcement or regulatory bodies, allows you to better manage the incident and collaborate to mitigate adverse effects. This cooperation reduces the risk of extensive damage and improves recovery.