To the CIO of Citibank,

The purpose of this evaluation is to assess the organization’s current cybersecurity performance through the lens of the NIST Cybersecurity Framework (Version 1.1). This assessment aims to determine the strengths and weaknesses of Citibank’s practices. Additionally, the evaluation will shed light on opportunities for improvement and offer recommendations to enhance the security maturity of the organization.

Before presenting the findings, it is important to understand the framework used for evaluation. For context, the National Institute of Standards and Technology Cybersecurity Framework (or NIST CSF for short) is a globally recognized framework designed to guide organizations in managing and mitigating cybersecurity risks. Version 1.1 of this framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover.

* **“Identify”** refers to an organization’s ability to comprehensively manage cybersecurity risks on systems, people, assets, data, and capabilities.
* **“Protect”** is the ability to limit and/or contain the impact of potential threats to the organization. This can be accomplished through access controls, training, data security, and so on.
* **“Detect”** is associated with the development and implementation of activities that identify cybersecurity events within a reasonable period. Examples of cybersecurity events may include ransomware, phishing, malware, and data breaches.
* **“Respond”** must be done as soon as a cybersecurity event is discovered. This function regards actions that will be taken by the organization to combat against the detected cybersecurity event.
* **“Recover”** is the process of returning to normal operations. The amount of time needed to recover depends on the impact of the cybersecurity event and the overall success of mitigations that were already in place.

The reason NIST CSF Version 1.1 was selected for evaluation was due to its flexibility and universal applications across industries of all sizes. To clarify, the framework tolerates unique customizations based on specific organizational needs in accordance with other standards such as ISO 27001, GDPR, and PCI DSS.

Th orchestration of the evaluation began by aligning the organization’s current security controls with the core functions and categories listed in the framework. Next, research was conducted on Citibank’s IT security teams, administrators, and other employees to assess the overall implementations and effectiveness of cybersecurity across the organization’s assets. A total of 118 implementations were evaluated using a maturity level ranging from 1-5. A rating of 1 signifies the lack or absence of cybersecurity, whereas a 5 represents the highest level of maturity in the given practice.

At the very least, organizations should aim for a maturity level of 3 across all core functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover). The maturity level of Citibank in terms of the framework can be seen below:

* **Identify –** 2.98 out of 5
* **Protect –** 2.93 out of 2
* **Detect –** 3.33 out of 5
* **Respond –** 3.56 out of 5
* **Recover –** 4 out of 5

From these results, it is evident the organization nearly meets a maturity level of at least a 3 across all core functions listed in the framework. The strongest area of strength can be seen in the organization’s recovery efforts in a cybersecurity event. From research, the implementation of a backup system whenever primary systems fail is highly effective in recovery efforts. Additionally, the existence of data replication mechanisms across global sites was noted. Given past cybersecurity events of the organization, the constant improvement in recovery strategies suggest a form of maturity that only manifests in organizations with experience and endurability.

The evaluation also provides significant data in Citibank’s response efforts. The maturity level of this core function was determined as a 3.56 out of 5. Although this rating is more than enough to reach the target level, the evaluation identified is a minor weakness in response improvements. Admittedly, it is difficult to update current strategies as technological advancements are fast and unpredictable. It is requested you consider additional investment of strategy updates by having the IT team monitor Common Vulnerabilities and Exposures (CVE) relevant to the assets used by the organization.

On the other side of the spectrum, the organization struggles to reach the target maturity level in terms of identifying cybersecurity risks and containing the impact of potential threats to Citibank. These categories received a maturity level of 2.98 and 2.93, respectively. Fortunately, these scores are within reach of the target maturity level, with the lower score reflected in the organization’s protection efforts. Significant challenges in central and remote maintenance of assets were discovered. Although there are policies in place that address asset management and remote access, the evaluation concludes that procedures are not properly documented and the lack of controls that would prevent access to unauthorized systems remotely. It is my recommendation you consult with your Chief Information Security Officer (CISO) for improved documentation and better implementation of access controls. You may reference the Principle of Least Privilege, which states users should be granted the minimum level of access necessary to perform their job functions. This would prevent unnecessary exposure to sensitive data or systems they don't require for their work. In the event a malicious user were to gain remote access to the organization’s assets, this principle would effectively safeguard sensitive information that should not be accessible to common employees.

The organization’s efforts in identifying cybersecurity risks are nearly enough to reach the target maturity level. Our evaluation noted an opportunity for growth in Citibank’s risk tolerance determination. It was found that despite several risk evaluation criteria exists, sector-specific analyses were informal. A suggestion would be to modify the current risk evaluation criteria to be analyzed by the sector roles in critical infrastructure and sector-specific risk analysis. Upon successful revision, the organization will reach the target maturity level recommended.

In summary, Citibank has demonstrated strong cybersecurity resilience, particularly in recovery and response capabilities, while areas such as protection and identification require minor improvements to meet target maturity levels. By addressing the identified gaps in asset management, access control, and risk evaluation, the organization will enhance its cybersecurity standing. Implementation of the recommended improvements will strengthen overall security and ensure Citibank remains adaptive/resilient in the ever-evolving threat landscape.