[redacted]
To: [redacted]
Subject: cyberframework
Date: Feedback regarding CSF 2.0 from BEYON Cyber
Attachments: Sunday, May 28, 2023 8:48:53 AM
image001.png
image002.png

Dear team,

As a student in the field of Cyber security and ardent follower of the NIST standards, it is my pleasure to submit my feedback regarding the current draft on behalf of Beyon Cyber:

1. Governance:
   The Governance domain is one of the most important additions to the framework. Especially as the governance in cyber security is such a complex task. I have proposed the following key areas to the domain in addition to those that are already mentioned:
   a. Add
   b. Cyber security mandate – The mandate translates the business objectives of the organization and shareholders into the security requirements. This is the first point of connection between business strategy and security outcomes.
   c. Clear Delegation of Authority that allows security functions to have the necessary authority to operate around its domain.
   d. Governance model highlighting the role of each entity within the scope of cyber security - this includes regulators, third parties, shareholders, etc.
   e. Cyber security metrics
   f. Roles and responsibilities
   g. Through life security involvement and oversight across all technology developments in the organization.

2. Risk measurement, sharing and reporting mechanism.
   a. In a complex integrated environment, interconnected and holistic risk management is necessary.
   b. For instance, currently STIX offers a way to communicate threat data however there is currently no mechanism to report Risk Data in a standard format.
3. Measurement of Risk:
   a. It is important to tie the strategic reporting metrics (at the strategy and business level) to operating metrics and KPIs - The two-way traceability as stated in SABSA architecture would be very useful to reference
4. Identify:
   a. It would be important to provide more guidance regarding threat intelligence sharing - especially as it is related to integrated risk management across entities that share the same threat ecosystem.
5. Detect:
   a. Important to consider the growing importance of cyber threat hunting.
6. Recover:

a. Important to consider the growing importance of forensics.

Regards,

BEYON
Cyber
Abubakar Mohd
GPCS,GPYC,CISSP, CISM, SABSA Architect,PMP, CRISC
Chief Technology Officer
[redacted]
beyoncyber.com