2. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: IDENTIFY

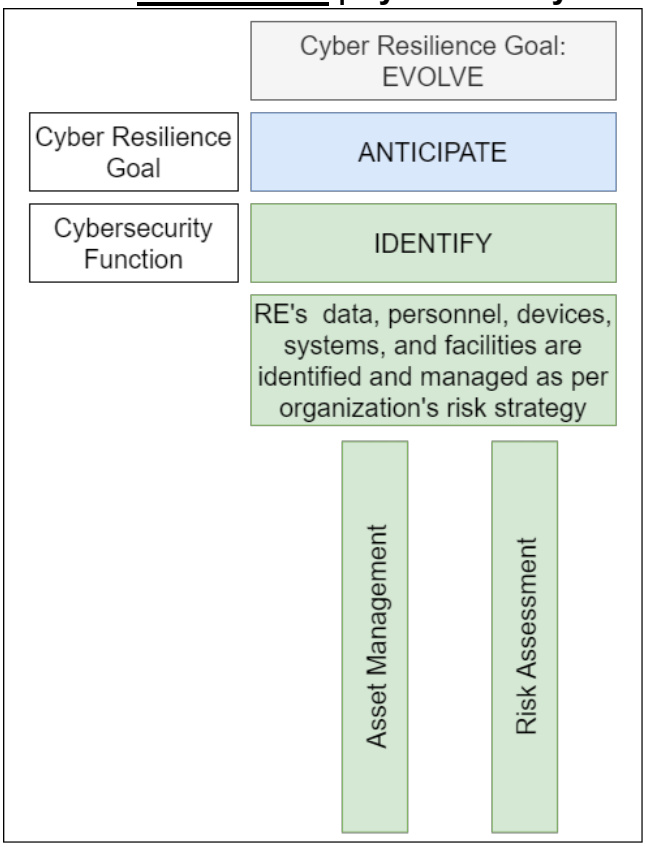

Figure 3: Overview of Identify function

2.1. ID.AM: Asset Management

i. ID.AM: Objective

The data, personnel, devices, systems, and facilities that enable the RE to achieve its business purposes are identified and managed consistently in accordance with their relative importance to organizational objectives and the RE's risk strategy.

ii. ID.AM: Standard

1. Physical devices, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets) and other interfacing systems within the organization are inventoried in a time bound manner.
2. Organizational communication, data flows and encryption methods shall be mapped and inventoried with respect to all IT systems and network resources.
3. REs shall ensure that no shadow IT assets are present in the organization.
4. Board/ Partners/ Proprietor shall approve the list of *critical systems*.
5. Inventories of data, and corresponding metadata for designated data types are maintained.

6. All inventoried IT assets and data are managed throughout their lifecycles.

2.2. ID.RA: Risk Assessment

i. ID.RA: Objective

The cybersecurity risk to the organization, assets, and individuals is assessed and understood by the RE.

ii. ID.RA: Standard

1. Asset vulnerabilities shall be identified, validated and documented. Risk factors shall be assessed and managed for all IT assets of the REs.
2. Risk assessment (including post-quantum risks[18]) of REs' IT environment shall be done on a periodic basis.
3. REs shall receive CTI from reliable/ trusted information forums and sources. REs shall be on-boarded to CERT-In Intelligence platform to receive the advisories for necessary action and implementation. Advisories issued by CERT-In/ CSIRT-Fin shall be implemented in a timely manner[19].
4. Threats, vulnerabilities, their likelihoods, and impacts shall be used to understand inherent risk and develop risk response prioritization. Vulnerabilities and cyber threats, especially related to access and authentication, along with their likelihood and potential business impacts, shall be identified and documented.
5. Risk responses shall be chosen, prioritized, planned, tracked, and communicated.

Box Item 7: Cybersecurity and Quantum Computing

Quantum Computers can efficiently break the asymmetric cryptographic systems which may jeopardize the security of transactions and expose sensitive data. Further, the symmetric cryptography may also require larger key sizes to remain secure. In view of the above, this may potentially be a major cybersecurity risk in the coming decade for the financial sector and for the REs.

To mitigate these risks, REs shall focus on the following indicative measures:

1. *REs shall maintain an inventory of cryptographic assets, prioritizing critical assets for Post Quantum Cryptography (PQC) migration, and assess their IT infrastructure capabilities.*
2. *REs shall develop strategies for the protection of assets which can and cannot be migrated to PQC.*
3. *REs shall upgrade employees' skills, periodically revise policies and conduct proof-of-concept trials in order to prepare themselves for cybersecurity challenges arising from quantum computing.*
4. *REs shall explore the feasibility to adopt PQC and technologies like Quantum Key Distribution (QKD).*

[18] Quantum computing is a rapidly emerging technology that exploits quantum mechanics' laws to solve complex problems. Post-quantum cryptography solutions can avert post-quantum risks and provide protection against quantum attacks.

[19] Within 24 hours of receiving or as indicated by SEBI.

5. *REs shall monitor ongoing quantum computing developments for cybersecurity threats, and ensure that senior management and relevant third-party service providers are aware of the possible risks associated with this technology.*
6. *REs shall enhance their crypto-agility to ensure a seamless transition to quantum-resistant solutions without disrupting their current IT systems.*