3. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: PROTECT

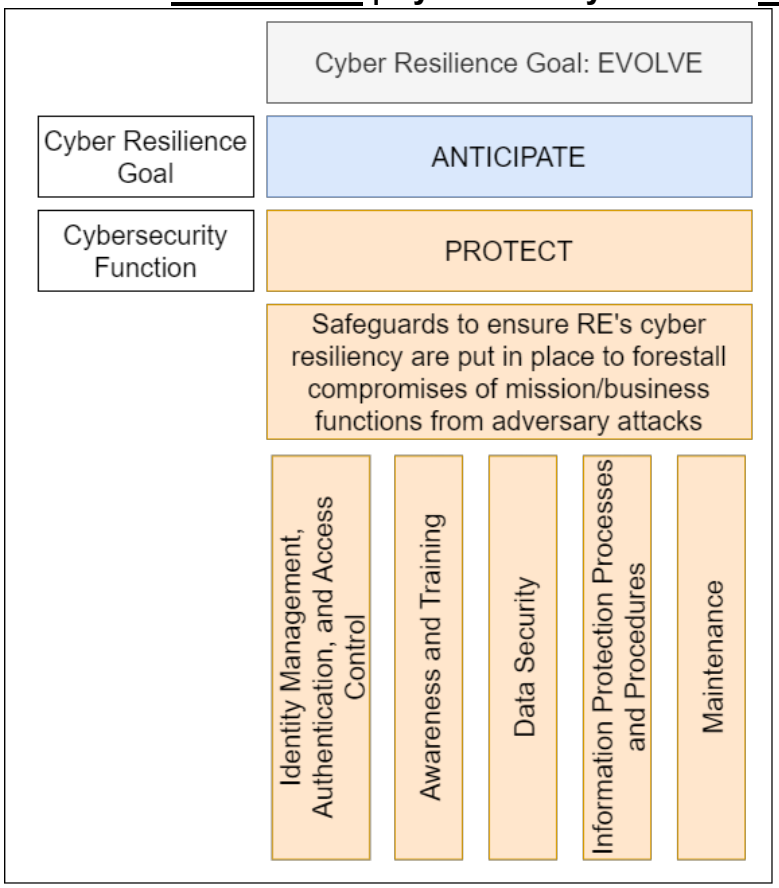

Figure 4: Overview of Protect function

3.1. PR.AA: Identity Management, Authentication, and Access Control

i. PR.AA: Objective

Access to physical and logical assets and associated facilities is limited to authorized users, processes and devices, and is managed commensurate with the assessed risk of unauthorized access.

ii. PR.AA: Standard

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
2. Network integrity is protected (through measures such as network segregation, network segmentation, etc.).
3. While granting access permissions and authorizations to resources (both on premise and cloud) of the organization, *Principle of Least Privilege* shall be followed along with segregation of duties.
4. REs shall follow Zero Trust Model to allow individuals, devices, and resources to access organization's resources.
5. Access rights shall be reviewed and documented on a periodic basis. Maker-Checker framework shall be implemented for granting, revoking, and modifying user rights in applications, databases, etc.
6. A comprehensive authentication policy shall be documented and implemented. Identities shall be proofed and bound to credentials and

asserted in interactions. Users, devices, and other assets are authenticated (single-factor or multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

7. All *critical systems* shall have MFA implemented for all users accessing from untrusted network to trusted network.
8. A comprehensive log management policy shall be documented and implemented.
9. User logs shall be uniquely identified and stored for a specified period.
10. Physical access to assets is managed, monitored, and protected. Physical access to the *critical systems* shall be monitored and recorded on a continuous basis. Individuals shall be screened before granting access to RE's organizational information and information systems.
11. Privileged users' activities shall be reviewed periodically. Access restriction shall be there for employees as well as third-party service providers. If it is required to grant access, it shall be for the limited time-period, on need-to-know basis and shall be subject to stringent supervision and monitoring.
12. Remote access to assets shall be strictly tracked and administered.
13. A comprehensive data-disposal and data-retention policy shall be documented and implemented.
14. Comprehensive SOPs shall be documented for handling storage media devices and their disposal.
15. Access control for using systems such as endpoint devices, networks, APIs, removable media, laptops, mobiles, etc. shall be defined and implemented.
16. Mobile applications shall be properly vetted against security requirements, and thoroughly tested before deployment.
17. API security with proper authentication and authorization mechanisms shall be defined and implemented.

Box Item 8: Application Programming Interface (API) security

Application Programming Interface: A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Application Programming Interface (API) is an interface that allows software applications to interact and communicate with each other using a set of definitions and protocols.

Since APIs have become key component of modern software application development, the practice of preventing or mitigating attacks on APIs has also become critical. API security refers to processes and solutions to mitigate vulnerabilities and risks in APIs. OWASP has released API Top 10 security threats after a sharp increase in API-related security threats.

API security guidelines broadly include the following categories:

1. ***API Discovery:*** *Knowing how many APIs are being exposed and what APIs are being used are critical steps in securing APIs.*
2. ***Access Management:*** *Enforcing strong authentication and authorization mechanisms enable secure verification of end-user client identity as well as limits the information access/ transfer to users/ systems. Implementing robust and reliable access management measures discourages use of open APIs, which*

increase the exposure and vulnerability of the data to potential breaches, fraud or misuse.

3. ***Rate Limiting:*** *Rate limiting and throttling protects bandwidth of the systems by enforcing a limit on how often an API is called and also prevents API abuse.*
4. ***Secure API development:*** *Incorporating secure-by-design strategy safeguards APIs and prevents misconfigurations and flaws.*
5. ***Zero-trust approach:*** *With zero-trust approach, API security assumes no implicit trust for any entity. Further, it also mitigates potential OWASP Top 10 API security risks.*

3.2. PR.AT: Awareness and Training

i. PR.AT: Objective

The RE's personnel and partners are provided cybersecurity awareness education, and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.

ii. PR.AT: Standard

1. Mandatory programs for building awareness of cybersecurity, cyber resilience, and system hygiene among employees shall be established. Such programs shall be conducted on a periodic basis, and shall be updated as per emergence of new threats, state-of-the-art technologies and industry trends.
2. REs shall ensure that privileged users understand their roles and responsibilities.
3. REs shall ensure that third-party stakeholders (e.g., suppliers, customers/ investors, partners) understand their roles and responsibilities.
4. REs shall ensure that senior executives/ Board members understand their roles and responsibilities. Further, a dedicated program on cybersecurity, cyber resilience, and system hygiene shall be made for Board members.
5. REs shall ensure that physical and information security personnel understand their roles and responsibilities.

3.3. PR.DS: Data Security

i. PR.DS: Objective:

Information and records (data) are managed consistent with the organization's risk strategy to protect the *Confidentiality, Integrity, and Availability* of information.

ii. PR.DS: Standard:

1. Data-at-rest and Data-in-transit shall be protected. Strong data protection measures (for both at-rest and in-transit data), with industry standard encryption algorithms, shall be put in place by all REs. Along with data-at-rest and data-in-transit, MIIs shall also explore solutions for encrypting data while it is being used/ processed.
2. REs shall classify their data into *Regulatory Data* and *IT and Cybersecurity Data* as defined in this framework. REs shall keep the *Regulatory Data* and *IT and Cybersecurity Data* available and easily

accessible in legible and usable form, within the legal boundaries of India.

3. Adequate capacity to ensure *Availability* of data shall be maintained.
4. Measures against data leaks shall be implemented. Appropriate tools shall be put in place to prevent any data leakage.
5. The development and testing environment(s) shall be separated from the production environment. For the development of critical software/ applications development, there shall be atleast one non-production environment to perform rigorous testing before deploying them to the production environment.
6. MIIs shall put in place integrity mechanisms to verify software, firmware, and information integrity of its *critical systems* and other systems connected to its *critical systems*.

Box Item 9: Data Classification

To ensure the smooth functioning of the securities market as well as sovereign control over data, SEBI has given high priority to security controls on the various kinds of data generated, managed, or processed by the REs. Taking this into consideration, CSCRF mandates REs to set up robust security controls for such data.
The data classification given below is technology agnostic, which will lead to a more enabled and strengthened environment for SEBI and REs.
CSCRF has defined the following categories of data:

1. ***Regulatory Data:*** *Regulatory Data includes the following (but not limited to):*
    a. *Data related to core and critical activities of the RE, as well as any supporting/ ancillary data impacting core and critical activities*
    b. *Data with respect to communication between investors and REs through applications (eg. chat communication, messages, emails etc.).*
    c. *Data that is required by the laws/ regulations/ circulars, etc. issued by SEBI and Govt. of India from time to time.*
    d. *Data that is deemed necessary or sensitive by the RE/ SEBI/ central or state government.*
    e. *The Regulatory Data shall be stored in an easily accessible, legible and usable form, within the legal boundaries of India. However, for the investors whose country of incorporation is outside India, the REs shall keep the original data, available and easily accessible in legible and usable form, within the legal boundaries of India. Further, if the copy retained within India is not in readable format, the REs must maintain an application/system to read/ analyse the retained data.*
2. ***IT and Cybersecurity Data:*** *IT and Cybersecurity Data includes the following data (but not limited to):*
    a. *Logs and metadata related to IT systems and their operations. However, such data should not contain the following:*
        i. *Any Regulatory Data, and*
        ii. *Sensitive data such as internal network architecture, vulnerability details, details of admin/ privileged users of REs, password hashes, system configuration, etc.*
    b. *Further, it should not be ordinarily possible to generate regulatory Data from IT and Cybersecurity Data.*

Box Item 10: Data Localization

SEBI functions to safeguard the interests of investors and promote the development of the securities market. This includes protecting the REs from all such risks which arise due to threats like single-point of failure, concentration risk, etc. While performing business activities, REs utilise services from third-party service providers. These

services include necessary software solutions hosted at the service providers' own and/ or third-party infrastructure. This could lead to business functions becoming more and more dependent on the service providers.
The hosted services/ software-as-a-service (SaaS)/ Cloud Service Providers (CSPs) usually store the data (business data, personal data etc.) where the processing of the data occurs. This results into data residing at the service providers' own and/ or third-party infrastructure.
While REs do not have a direct control on where their data is stored by the service providers, it is important to note that the REs' data may be stored on servers outside the legal boundaries of India.
If the REs' data resides outside the legal boundaries of India, SEBI and its REs may not have sovereign control on it which may cause governance issues and put limitations on the compliance of various laws related to data protection and cybersecurity in the country.
In order to protect interests of investors, and SEBI REs and their businesses, SEBI has envisaged data localization. Data localization means that all the data generated (including creation and storage) within the legal boundaries of India remains within the legal boundaries of India. Data localization ensures data sovereignty and data residency together. It will also lead to better governance and oversight.
SEBI REs shall ensure that processing and storage of data is done within legal boundaries of India. CSCRF has mandated REs to keep the original Regulatory Data available and easily accessible in legible and usable form, within the legal boundaries of India. However, for the investors whose country of incorporation is outside India, the REs shall keep the original Regulatory Data, available and easily accessible in legible and usable form, within the legal boundaries of India. Further, if the Regulatory Data retained within India is not in readable form, the REs must maintain an application/ system to read/ analyse the retained data. However, the IT and Cybersecurity Data which is to be sent to/ consumed by global/ international SOC of the REs, and SaaS based cybersecurity solutions, has been exempted from being maintained within the legal boundaries of India. For the above-mentioned SaaS based cybersecurity solutions and SOC offerings utilized by the REs (where the data is not processed/ stored within the legal boundaries of India), the IT and Cybersecurity Data sent to such solutions shall be classified, assessed and periodically reviewed (at least once in a year) by the respective IT Committee for REs or equivalent body of the RE. Additionally, such IT and Cybersecurity Data shall be approved by the Board/ Partners/ Proprietor annually.

3.4. PR.IP: Information Protection Processes and Procedures

i. PR.IP: Objective:

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

ii. PR.IP: standard:

1. A baseline configuration of IT systems shall be created and maintained incorporating security principles (e.g. concept of least functionality).
2. A System Development Life Cycle to manage systems shall be implemented.
3. REs shall put in place processes for configuration change control as well as change management.
4. REs shall thoroughly scan Critical software/ applications to ensure that no malicious code is present.

5. If the source code of software/ application is not owned by the REs, then in such a case, the REs shall obtain an undertaking/ certificate from the third-party service providers stating that their software/ application is free of known vulnerabilities, malwares, malicious/ fraudulent code and any covert channels.
6. Testing/ certification of software/ applications shall broadly address the objectives such as product/ version/ module(s) functions only in a manner that it is intended to do, it is developed as per the best secure design/ coding practices and standards, it addresses known flaws/ threats due to insecure coding, etc.
7. REs shall document backup and recovery plan of data to ensure that there is no data loss.
8. REs shall implement, test, and maintain data backups. Further, drills for restoration of backup data shall be conducted on a periodic basis.
9. Policies and regulations regarding the physical operating environment for REs' assets shall be defined and adhered to.
10. Effectiveness of protective technologies shall be measured on a regular basis in line with the SLAs.
11. Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) shall be put in place and regularly tested and updated.
12. A vulnerability management plan shall be developed and implemented.
13. For applicable cloud instances of REs, SEBI circular '*Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)*' shall be complied with.
14. Only CERT-In empanelled IS auditing organizations shall be onboarded for external audit (including cyber audit) of REs to audit the implementation of standards and mandatory guidelines (as applicable) mentioned in this framework.
15. All software services in the form of SaaS/ Hosted services, COTS, customized COTS, in-house developed software, etc. shall be certified for application security and functional audit. COTS products empanelled by stock exchanges/ depositories shall be certified for application security testing, and functional audit by STQC at the time of empanelment.
16. MIIs and Qualified REs shall obtain ISO 27001 certification.
17. MIIs and Qualified REs shall follow globally recognized standards such as CIS Critical Security Controls to enhance their cyber resilience.

3.5. PR.MA: Maintenance

i. PR.MA: Objective:

Maintenance and repairs of organizational control and information system components are performed consistent with policies and procedures.

ii. PR.MA: Standard:

1. Maintenance and repair of REs' assets shall be performed and logged, with approved and controlled tools.
2. Remote maintenance of REs' assets shall be approved, logged, and performed in a manner that prevents unauthorized access.
3. Patches shall be identified and categorized based on their severity. Critical patches shall be implemented at the earliest. Patches shall be tested in non-production environment before applying to DC and DR.