Definitions

1. **CIA triad[6]:**
   a. **Confidentiality:** Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.
   b. **Integrity:** Property of accuracy and completeness.
   c. **Availability:** Property of being accessible and usable on demand by an authorised entity.

2. **Critical Systems –**
   Entities shall identify and classify their critical IT systems. Following systems shall be included in critical systems (both on premise and cloud):
   a. Any system, if compromised, that will have an adverse impact on core and critical business operations.
   b. Stores/ transmits data as per regulatory requirements.
   c. Devices/ network through which critical systems are connected (through trusted channels).
   d. Internet facing applications/ systems.
   e. Client facing application/ systems.
   f. All the ancillary systems used for accessing/ communicating with critical systems either for operations or for maintenance.

3. **Cyber Capability Index (CCI) –**
   CCI is an index applicable for MIIs and Qualified REs which is calculated based on certain parameters as specified in this framework. The purpose of CCI is to ascertain the cyber resilience capabilities of MIIs and Qualified REs and their maturity in terms of implementation of cybersecurity measures.

4. **Cyber Event –**
   Any observable occurrence in an information system. Cyber events sometimes provide indication that a cybersecurity incident is occurring. – *FSB Cyber Lexicon*[7]

5. **Cyber Resilience –**
   The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents. – *FSB Cyber Lexicon*[8]

[6] https://www.fsb.org/wp-content/uploads/P130423-3.pdf
[7] https://www.fsb.org/wp-content/uploads/P130423-3.pdf
[8] https://www.fsb.org/wp-content/uploads/P130423-3.pdf

6. **Cyber Threat –**
   A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity. – *FSB Cyber Lexicon*[9]

7. **Cybersecurity Incident (Incident)–**
   Any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes in data, information without authorisation. – *CERT-In Cybersecurity directions*[10]

8. **Hosted Service -**
   Any IT/ SaaS provider rendering IT services/ SaaS solutions hosted on IT infrastructure either owned or controlled and managed by the service provider shall be broadly construed as hosted services. Hosted services have to fulfil the following technical specifications:
   1. Data center that hosts IT services/ SaaS solutions shall be ANSI/ TIA-942 rated-4 standard certified or equivalent (e.g. Tier 4) with complete fault tolerance and redundancy for every component.
   2. IT infrastructure shall atleast be of equivalent standard of MeitY Empanelment of Cloud Service offerings of Cloud Service Providers (CSPs) and audited by a STQC empanelled cloud audit organisation or equivalent established international agency.
   3. Summary of VAPT reports shall be made available to the REs and to the SEBI on demand.
   4. If the data center is operated from outside the legal boundaries of India, then a copy of REs' data in human/ application readable form shall be maintained within the legal boundaries of India.
   5. Hosted service provider shall ensure that there is no "*Kill Switch*" available in the Application, which would remotely disable the functioning of the solution.
   6. There shall be an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (including but not limited to technical, managerial, governance related, etc.) of the hosted services between the RE and Hosted service provider. The aforementioned delineation of responsibilities shall be added explicitly in the agreement (as an annexure) signed between the RE and the CSP. For details refer to "*Framework for adoption of cloud services for SEBI Regulated Entities*".

[9] https://www.fsb.org/wp-content/uploads/P130423-3.pdf
[10] Refer Q 3. In CERT-In Cybersecurity directions: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

9. **ISO 27001 certification[11] –**
   ISO 27001 certification is a globally recognized standard for Information Security Management Systems (ISMS) published by the International Organization for Standardization (ISO). It helps organizations become risk-aware, proactively identify, and address weaknesses and promote a holistic approach to information security.

10. **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.

11. **Major Change/ Major Release**
    CSCRF has mandated VAPT after every major release. The following changes (including but not limited to) are broadly considered as major release(s) or major change(s):
    a. Implementation of a new SEBI circular.
    b. Changes in core versions of software (e.g., .net, SQL, Oracle, Java, etc.)
    c. Any changes in policy of login and/ or password management.
    d. Significant system modifications that alter how data is exchanged with stock exchanges (e.g., file format changes, message protocol changes, etc.).
    e. Introduction of new security protocols (e.g., switching from SSL to TLS 1.3).
    f. Expansion into new financial markets (e.g., adding currency trading).
    g. Implementation of new processes/ schema changes.

12. **Market Infrastructure Institutions (MIIs) –**
    Stock Exchanges, Depositories and Clearing Corporations or any other institutions as specified by SEBI are collectively referred to as Market Infrastructure Institutions (MIIs). For applicability and inclusion of REs as MIIs, refer to section 2 ("*Thresholds for REs' categorization*") of CSCRF.

Box Item 1: REs under MIIs category for compliance with CSCRF

In the context of CSCRF, following REs are constituted as MIIs:

1. *Stock Exchanges*
2. *Depositories*
3. *Clearing Corporations*
4. *KRAs*
5. *QRTAs*

All the circulars issued by SEBI on cybersecurity for MIIs shall be uniformly applicable to all the above REs.

[11] https://www.iso.org/standard/27001

13. **Principle of Least Privilege (PoLP) –**
    Principle of Least Privilege (PoLP) is an information security concept which maintains that a user or entity shall only have access to the specific data, resources and applications needed to complete its required task.

14. **Red team exercise –**
    An exercise, reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organizational missions or business processes and to provide a comprehensive assessment of the security capabilities of an organization and its systems.

15. **Regulated Entity (RE)[12] -**
    The term 'Regulated Entity' refers to SEBI registered/ recognised intermediaries (for example stock brokers, mutual funds, KYC Registration Agencies, QRTAs, etc.) and Market Infrastructure Institutions (Stock Exchanges, Depositories and Clearing Corporations) regulated by SEBI.

16. **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 w.r.t to communication between investors and REs through applications (e.g., 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 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 saved data.

17. **Risk –**
    As defined by OWASP[13], Risk = Likelihood × Impact; where Likelihood = Threat × Vulnerabilities. Likelihood is a measure of how likely a vulnerability is to be discovered and exploited by an attacker. Impact is the magnitude of harm that can be expected as a result from the consequences of threat exploitation.

[12] Entities within SEBI's purview, refer to Securities Contracts (Regulation) Act 1956, SEBI Act 1992, and Depositories Act 1996.
[13] Refer Risk-rating methodology: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

18. **Risk-based Authentication (RBA) –**
    Risk-based authentication is a non-static authentication mechanism that takes into account the profile of the agent requesting access to the system to determine the risk profile associated with that transaction. It checks and applies varying levels of stringency to authentication processes based on the likelihood that access to a given system could result in it being compromised.

19. **Root Cause Analysis (RCA) –**
    A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.

20. **Secure Software Development Life Cycle (SSDLC) –**
    Secure Software Development Life Cycle (SSDLC) involves integrating security testing at every stage of software development, from design, to development, to deployment and beyond.

21. **Software Bill of Materials (SBOM) –**
    A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.

22. **Trusted Channels –**
    A protected communication link established between the cryptographic module and a sender or receiver (including another cryptographic module) to securely communicate and verify the validity of plaintext CSPs, keys, authentication data, and other sensitive data. It is also called a secure channel.