client alert

September 04, 2024

cyril amarchand mangaldas
ahead of the curve

The SEBI Comprehensive Cybersecurity and Cyber Resilience Framework: The New Rules of the Road

The Securities and Exchange Board of India (**SEBI**) has issued a comprehensive Cybersecurity and Cyber Resilience Framework (**CSCRF**) applicable across all Regulated Entities (**REs**)[1]:

1. Alternative Investment Funds,
2. Bankers to an Issue and Self-Certified Syndicate Banks;
3. Clearing Corporations;
4. Collective Investment Schemes;
5. Credit Rating Agencies;
6. Custodians;
7. Debenture Trustees;
8. Depositories;
9. Designated Depository Participants;
10. Depository Participants through Depositories;
11. Investment Advisors/ Research Analysts;
12. KYC Registration Agencies;
13. Merchant Bankers;
14. Mutual Funds / Asset Management Companies;
15. Portfolio Managers;
16. Registrar to an Issue and Share Transfer Agents;
17. Stock Brokers through Exchanges;
18. Stock Exchanges; and
19. Venture Capital Funds.

Prior to the CSCRF, cybersecurity obligations under diverse circulars were applicable in respect of Market Infrastructure Institutions (**MIIs**), Stockbrokers, Depository Participants, Mutual Funds/ Asset Management Companies, KYC Registration Agencies, Qualified Registrar to an Issue and Share Transfer Agents, and Portfolio Managers.

In addition to superseding prior circulars the CSCRF consolidates requirements on cybersecurity and cyber resilience, applicable to REs, in one comprehensive framework.

Consequently, while some contents of the CSCRF are not entirely unfamiliar to some REs, material changes and new obligations with significant consequences for all of them, means that the CSCRF will have material impact for them all. The CSCRF is also innovative in terms of how it perceives cybersecurity risk and governance. For instance:

a. It expressly requires risk assessments to provide for post quantum risk.

b. It imposes obligations on boards of REs to be actively involved in matters such as identifying critical systems, classifying data, and confirming key obligations.

1 SEBI | Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)

Classification of Regulated Entities

The CSCRF adopts a graded approach and regulates REs based on their size, scale, span of operations and certain thresholds like number of clients, trade volume, asset under management in the previous financial year.

REs can be classified into one of the five categories: a.) MIIs; b.) Qualified REs; c.) Mid-size REs; d.) Small-size REs; and e.) Self-certification REs.

While some of these definitions include objective thresholds, other's such as the definition of Qualified RE in merchant banking, are less clear, and notionally extent to "significant" REs.

Once categorised, the RE would remain in such category throughout the financial year. Where an RE holds more than one license, and consequently falls within more than one category of REs, compliance for the highest category would be applicable.

Key compliances under CSCRF

Data Localisation

Much of the recent discussion around the CSCRF, and its perceived disruptive effect surrounds the broadly worded data localization norms its includes.

REs are required to categorise data into Regulatory Data and IT & Cybersecurity Data as follows:

Regulatory Data	IT & Cybersecurity Data
Regulatory Data should include all data related to **core and critical activities** and supporting or ancillary data. It also expressly include data relating to communication between investors and REs through applications, and data that is required by laws	IT and Cybersecurity Data includes logs and metadata relating to the IT systems and their operations, but cannot include, or be used to generate Regulatory Data.

REs are required to store Regulatory Data in an easily accessible, legible and usable form, **within the legal boundaries of India**. Where data is not in readable format, REs are required to maintain applications or systems to read retained data.

IT and Cybersecurity Data, which is to be sent to/ consumed by an international Security Operation Centre of the REs, and Software as a Service based cybersecurity solutions, is exempt from being maintained within the legal boundaries of India, subject to periodical review and being made available in forty eight (48) hours.

Vulnerability Assessment & Penetration Testing (VAPT)

VAPT has to be conducted after every major release which includes implementation of a new SEBI circular and changes in core versions of software, policy pertaining to login/ password management, system modification in how data is exchanged with stock exchanges, security protocols, expansions into new financial markets and implantation of new processes/ schema changes. REs have to plan their VAPT activity in the first quarter of the financial year and have to ensure that no audit cycle is left unaudited (if any) due to the change in category.

Other Important Compliances

Some of the other important compliances that REs have to carry out are as under:

a. MIIs and Qualified REs have to designate a senior official as Chief Information Security Officer (**CISO**).

b. MIIs and Qualified REs have to obtain the source codes for all critical applications from the third-party service providers.

c. REs (other than self-certification REs) to engage only Indian Computer Emergency Response Team (**CERT-In**) empanelled Information Security auditing organizations for conducting external audits including cyber audit.

d. REs are required to develop an Incident Response Management Plan.

e. Cyber attacks, cybersecurity incidents and/ or breach to be notified to SEBI and CERT-In within (6) Six hours of noticing/ detecting such incident or being brought to notice about such an incident.

f. In case of disruption of any one or more of their critical systems, REs have to declare the incident as a 'Disaster' based on the business impact analysis, within (30) Thirty minutes of the incident.

Implementation of CSCRF

A glide path has been provided whereby:

a. Stock Brokers, Depository Participants, Mutual Funds / Asset Management Companies, KYC Registration Agencies, Qualified Registrar to an Issue and Share Transfer Agents, and Portfolio Managers are required to comply with the CSCRF by January 01, 2025; and

b. Other REs are required to comply with the CSCRF by April 01, 2025.

Challenges to Implementation

Several key aspects that include issues as fundamental as the definition of 'regulatory data', which include all communication with investors may pose challenges in international transactions and deal making and have material consequences on the businesses of REs. Further, transfer and processing of data outside India may be necessary to enable AML/ KYC/ Sanctions check, fraud prevention and detection, compliance and conflict avoidance as well as global research and advisory activities. The REs would have to engage with their counter parties, cybersecurity auditors and the regulator in respect of the specifics of the obligations arising out of CSCRF, especially considering the short timelines provided for implementation of the CSCRF.

Engagement with the regulator may be required regarding the specifics of the CSCRF. It is, however, quite clear that data sovereignty, cybersecurity and associated risk mitigation is going to be a core focus for the regulator. Specific responsibilities have been placed on the Board/ Partners/ Proprietors and it is likely that any non-compliance may be viewed seriously by the regulator.

Key contacts

Cyril Shroff
Managing Partner
cyril.shroff@cyrilshroff.com

Arun Prabhu
Partner (Head - Technology)
arun.prabhu@cyrilshroff.com

Vasudha Goenka
Partner
vasudha.goenka@cyrilshroff.com

Sangram Mallick
Principal Associate
sangram.mallick@cyrilshroff.com