8 August 2023

To:
Ms. Shweta Banerjee (DGM-ITD)
SEBI Bhavan II BKC
Plot no. C-7, 'G' Block, Bandra Kurla Complex
Bandra (E), Mumbai (Maharashtra)-400051

RE: ASIFMA Response to SEBI Consultation on 'Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities'

Dear Ms. Shweta Banerjee,

On behalf of the Asia Securities and Financial Markets Association ("ASIFMA")[1] members, we are reaching out to engage with you in relation to the Securities & Exchange Board of India ("SEBI") '*Consultation Paper on Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities*' ("Consultation Paper") that was issued on 4 July 2023 and outlined the draft master framework on cybersecurity and cyber resilience.

We would like to again express our gratitude and thankfulness for SEBI's extension to the submission deadline and kind invitation to ASIFMA to have the opportunity to attend and participate in the 18 July 2023 discussion meeting, discuss the consultation paper, and hear from the Regulated Entities ("REs") and stakeholders on their thoughts, inputs, and suggestions, to the Circular.

Members have collectively reviewed the Consultation Paper and would like to raise the following operational challenges and concerns with respect to some of the requirements as listed below. Members have also provided some suggested alternative approaches and suggestions they would like to respectfully recommend SEBI to kindly review, which can also achieve the intended objectives whilst strengthening the sector's cybersecurity posture.

Suggestions and recommendations:

1. **Criteria and Scope of Critical Systems**
   1.1. Consider aligning with Reserve Bank of India's framework that allows REs to have their own framework/criteria for identifying critical assets.

   1.2. Recommend that the scope of 'critical assets' to refer to '*critical systems that will cause significant disruption to operations or materially impact the REs' services to its customers.'*, E.g., a system that (a) processes transactions that are time critical; or (b) provides essential services to customers.

2. **Remediation Timelines for Vulnerability Assessment and Penetration Testing ("VAPT") and Cyber Audit findings**

[1] *ASIFMA is an independent, regional trade association with over 170 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.*

2.1. The industry recognises SEBI's efforts to strengthen the sector's cybersecurity posture. However, the proposed three months remediation timelines for findings from the VAPT/Cyber Audit activities prove quite challenging for REs to meet, especially if a particular vulnerability requires engaging vendors and changing of the source code.

2.2. Members would like to suggest a '*graded approach'* for remediation be adopted, so that REs could develop resolutions based on the graded level of risk and impact.

2.3. Members would like to suggest for SEBI to recognise the risk acceptance approach based on the RE's Risk Management Framework, in line with Objective 1.1.1(e) of the Framework.

3. Risk Assessment Framework, Scope, and Frequency

3.1. We suggest that the draft framework allows firms which currently leverage existing risk assessment frameworks, such as the Cyber Risk Institute Profile or the NIST Cybersecurity Framework, to fulfil the risk assessment in this draft Framework against those recognized frameworks and ensure the gaps between the existing frameworks and SEBI framework are bridged.

3.2. Members have concerns that the current half-yearly review requirement is overtly too frequent as firms' cyber risk management practices do not change dramatically over 6 months. We would suggest SEBI consider an assessment period of every 2 to 3 years, similar to other APAC jurisdictions like Hong Kong.

4. Periodicity for other reviews (aside from risk assessment)

4.1. Under the requirements, it requires that user access rights and password reviews be completed quarterly, review of third parties' management of systems half-yearly, drills and recovery plan assessments every quarter.

4.2. Members proposed an alternative approach whereby firms could take a '*risk-based approach*', or alternatively, a consideration in alteration of frequency of the reviews to at least annually. There are concerns that the quarterly or half-yearly reporting would be overly onerous for firms and may not be meaningful since not much change would have occurred over such a short period.

5. Reporting of cyber incidents to be 'actual' cybersecurity incidents with material impact

5.1. We recommend that 'cybersecurity incidents' be defined as an occurrence that:

5.1.1. Results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits;

5.1.2. Constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies; and

5.1.3. Materially impact operations and customers.

5.2. We recommend that the 6-hour reporting be triggered when there is evidence of a Cybersecurity safeguard failure that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. Reporting timeline should not be counted from when the firm '*notices*' the incident, as the event may not result in any '*actual incident'*, and as a result may lead to overreporting.

6. 2-hour recovery time objective ("RTO") and 15 minutes recovery point objectives ("RPO")

6.1. The Bank of England recently published the results of its inaugural cyber stress test in which it acknowledged that "*there might be instances where the disruption caused by an incident was such that, despite prior planning, attempting to recover by the end of the value date could*

have a more adverse impact on financial stability than failing to do so."[2] For e.g., for cases where recovery times were mandated for tail events and non-standard failure scenarios.

6.2. There is a concern that '*mandated recovery times*' not contemplating for feasibility or practicality under a range of disruptions, could cause organisations to prioritise recovery time over safety. Members recommend the RTO and RPO be determined by REs on a risk-based approach.

6.3. **Cybersecurity scenario based RPO/RTO table *(Annexure D)*** - members would like further clarity and details on the asks and expectations regarding the output/response to the table.

7. Alignment of 'Specified REs' to the criteria of Qualified Stockbrokers ("QSB")

7.1. Recommend to align the criteria of 'specified REs' to the existing criteria used for QSBs so as to allow for consistent implementation.

8. Further clarification / suggestions on requirements

8.1. **Implementation period** – as the framework is rather comprehensive and many of the requirements require new controls/enhancements to current controls, hence will require sufficient time for remediation and implementation. We respectfully suggest SEBI to allow a 2-year grace period for implementation.

8.2. **Software Bill of Materials (SBOM)** - the industry has not yet reached the level of maturity required in this Consultation Paper, and, therefore, we suggest for the SBOM under section 1.4.3(a)(ii) to remain as an optional recommendation.

8.3. **Authentication policy** - as more organisations move towards '*password-less*', members suggest SEBI refer to the authentication policy in place of password policy under section 2.1.3(a)(i).

8.4. **Multi factor authentication (MFA)** – members suggest that under section 2.1.2(b) "*critical systems shall have MFA implemented for all users*", that only access to critical systems over the internet/online facility shall have MFA implemented for all users.

8.5. **Password policy** – members suggest that section 2.1.3(a)(i)(8) be an optional recommendation as many organisations utilise systems that implement one-way hash, where ex-employees' passwords are unable to be decrypted and compared.

8.6. **Physical security** – members suggest using the wording "*physical access to Data Centres hosting critical systems*" under section 2.1.3(a)(iii) for clarity.

8.7. **Vulnerabilities remediation** - members suggest that vulnerabilities remediation based on best practices baselines such as OWASP and CWE/SANS are limited to critical software/application as mentioned in section 2.4.3(a)(4).

8.8. **Depositary Circulars** - members encourage SEBI to guide depositories to also make an effort to streamline their Circulars and Advisories based on the SEBI Circulars (listed on pg. 16) will be withdrawn.

8.9. **Framework override over previous Circulars** - clarification whether the SEBI Circular dated February 2023 on Advisory on Cyber Security Best Practices will supersede and be overwritten by this new framework.

8.10. **Measuring and auditing SOC functional Efficacy *(Annexure M)*** - with respect to the Annex M (pg. 115) requirement, '*Measuring and auditing functional efficacy of SOC'*, to date there has yet to be any global precedent of this type of regulatory requirement, therefore, members would like to further understand SEBI's purpose and objectives of this requirement,

[2] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test.pdf

and how the quantifiable calculations would be measured, before mandating REs to fulfil the requirements.

8.11. **Log management and Log retention** - *"All REs shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs shall be maintained and stored in a secure location for a time period not less than two (2) years".* Members propose to have this requirement of log management and log retention be in line with the CERT-In directions issued on 28 April 2022, they state that logs should be maintained securely for a rolling period of 180 days.

8.12. **Forensic and root cause incident analysis** - performing forensic and root cause analysis for all types of incidents could prove rather challenging and time-consuming for REs, members suggest for SEBI to establish criteria to identify which incidents they believe would require forensic and root cause analysis.

8.13. **VAPT**

8.13.1. **VAPT frequency** - members suggest allowing firms to conduct VAPT during the financial year, rather than restricting the timeline as specified, to being the first quarter of every financial year. VA scans are performed regularly; however, PT requires year-long projections and planning in terms of budget and resources, members would be grateful if SEBI allowed for sufficient time to plan accordingly.

8.13.2. **VAPT scope** - members note that the scope for VAPT is rather broad and restricts REs from employing a graded approach with respect to testing of its most critical assets. Members respectfully suggest SEBI allow firms to define the assets in scope for VAPT according to risk informed methodologies.

8.13.3. **CERT-IN-empaneled vendors** - for Global systems hosted externally to India, members suggest that testing results from independent, non-CERT-IN-empaneled vendors be accepted to meet VAPT requirements specified in this framework.

Once again, we are grateful for the kind extension in submission timeline and appreciate the opportunity to share our views with SEBI. We humbly request SEBI to kindly review the concerns and suggestions aforementioned. ASIFMA and its members are keen to engage with you on this important topic and stand ready to further discuss the Circular at your convenience.

Please do not hesitate to reach out to myself Laurence Van der Loo, at lvanderloo@asifma.org for any questions. In the meantime, we remain at your disposal if you wish to discuss any further details.

We look forward to your reply.

Yours sincerely,

Laurence Van der Loo
Executive Director, Technology and Operations
Asia Securities Industry and Financial Markets Association (ASIFMA)