Summary: DSCI's Submission on SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF)

The Data Security Council of India (DSCI) submitted detailed inputs on SEBI's Consultation Paper on the Consolidated Cybersecurity and Cyber Resilience Framework (CSCRF), released in July 2023. While supporting SEBI's efforts to strengthen cybersecurity in the capital markets ecosystem, DSCI's feedback seeks to ensure that the framework is risk-based, innovation-friendly, technically sound, and operationally feasible for Regulated Entities (REs), including Market Infrastructure Institutions (MIIs).

Some of the key suggestions advanced by DSCI included

1. **Definition of Critical Assets**

DSCI highlighted that the draft definition of "critical assets" is overly broad, encompassing nearly all IT systems and interconnections, which could overwhelm organizations.

Based on that apprehension, DSCI suggested narrowing the definition to include only those systems that are truly vital to the continuity and integrity of services. A risk-based approach should guide classification to avoid resource dilution.

2. **Asset Inventory Management**

The draft mandated updating asset inventories within 24 hours, which may be impractical for large or cloud-native infrastructures.

DSCI advocated for some flexibility by requiring inventories to be "kept up to date" rather than enforcing a rigid timeline. Focus on critical assets and explore modern cloud-based discovery mechanisms.

3. **Clarity in Governance Roles**

The roles of Designated Officer and CISO were not clearly distinguished in the CSCRF. DSCI recommended to provide explicit guidance on the responsibilities and hierarchical placement of these roles to ensure clarity and prevent governance overlaps.

4. **Third-Party and Supply Chain Risk Management**

It was also observed that the obligations on third-party service providers (TSPs) are prescriptive and may not align with practical outsourcing models.

DSCI recommended to adopt a principle-based approach, encouraging REs to assess and manage supply chain risk without imposing unrealistic uniform standards. Recognize equivalent certifications like ISO 27001 in lieu of mandated SEBI-specific audits.

5. **Incident Reporting Timelines**

DSCI highlighted that the requirement in the draft framework to report incidents to SEBI within 6 hours duplicates the CERT-In mandate and is operationally burdensome, especially during incident response.

DSCI suggested alignment of SEBI's reporting requirement with CERT-In's 72-hour framework. Use the 6-hour window only for CERT-In and define "significant incidents" more clearly to avoid over-reporting and resource strain.

6. **Log Management and Retention**

The framework requires a two-year log retention period and mandates logs be stored in India, which conflicts with CERT-In's direction of 180 days and flexibility on log location. Highlighting this ambiguity, DSCI suggested alignment of retention timelines with CERT-In's 180-day rule. Allow logs to be stored outside India with the condition that REs must provide logs upon request.

7. **Operational Resilience vs. Concentration Risk**

DSCI in its observation shared a concern that the draft framework overemphasizes concentration risk in outsourcing, which may discourage use of best-in-class services. In its submission DSCI suggested SEBI to shift focus from "concentration risk" to "operational resilience", ensuring REs have contingency plans rather than limiting vendor choices.

8. **Security of Cloud and Off-the-Shelf Products**

DSCI highlighted that mandating Common Criteria EAL 4 certification for software products may hinder adoption of emerging and startup-led technologies. It recommended that the draft framework may avoid mandating this certification and instead rely on the broader cybersecurity controls already outlined in CSCRF. Recognize the practical limitations for vendors, especially startups.

9. **Audit Requirements and Empanelment**

It was observed that restricting the external audits to CERT-In empanelled auditors and enforcing a 3-year cooling-off period may lead to capacity bottlenecks and logistical challenges. The recommendation was to make this requirement mandatory only for MIIs. Allow other REs to engage with globally accredited audit bodies and introduce flexibility in audit cycling requirements.

10. **Confidential Computing and Data Security in Use**

Mandating "confidential computing" for data protection is premature due to lack of maturity and industry adoption. The recommendation was to use the term 'data security

in use' and clarify that it is recommended (not mandatory). Allow evolving technologies to mature before mandating their use.

11. Vulnerability Assessment and Penetration Testing (VAPT)

It was also brought into the submissions that the uniform approach to the VAPT may not suit the wide diversity of REs and technology stacks. Hence it was suggested to allow flexibility in VAPT frequency based on system criticality. Encourage REs to automate vulnerability assessments while scheduling penetration testing as per risk level.

Conclusion

DSCI welcomes SEBI's initiative to unify and strengthen cybersecurity practices across the securities market. Its submission urges a balanced approach—combining robust controls with operational flexibility, alignment with existing national regulations (like CERT-In), and global best practices.

By incorporating these suggestions, SEBI can ensure that the CSCRF not only enhances cyber resilience but also supports innovation, eases compliance, and reinforces India's standing as a secure and forward-looking digital economy.