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

October 2024

# Foreword



In today's rapidly evolving cybersecurity landscape, the Securities and Exchange Board of India (SEBI) has made a significant advancement with the introduction of the "Cybersecurity and Cyber Resilience Framework (CSCRF)" on August 20, 2024. More than just a regulatory directive, this framework represents a comprehensive strategy aimed at fortifying the defences of SEBI-regulated entities against the growing wave of cyber threats that endanger the integrity and trust of India's financial systems. Through CSCRF, SEBI reinforces its commitment to embedding cybersecurity into the very foundation of every regulated entity, fostering robust and resilient financial markets in India.

The CSCRF framework categorizes regulated entities based on their size, operational complexity, and risk profile, enabling the adoption of customized cybersecurity measures. Its key components include governance structures, incident response protocols, risk management strategies, and rigorous third-party vendor assessments. A defining feature of the framework is the introduction of the "Cyber Capability Index (CCI)," which reflects SEBI's dedication to continuously assessing and enhancing cybersecurity maturity throughout the sector. Additionally, major exchanges such as NSE and BSE have already established Security Operations Centers (SOCs) to provide crucial support to smaller entities, highlighting the importance of collaboration in the fight against increasingly sophisticated cyber threats.

In this publication, we provide an in-depth perspective on the CSCRF 2024, examining its requirements and the strategic approach necessary to meet them. We will explore how organizations can align with SEBI's CSCRF, adhere to compliance timelines, and develop a robust cybersecurity posture that not only safeguards operations but also fosters confidence among stakeholders.

Yours sincerely,

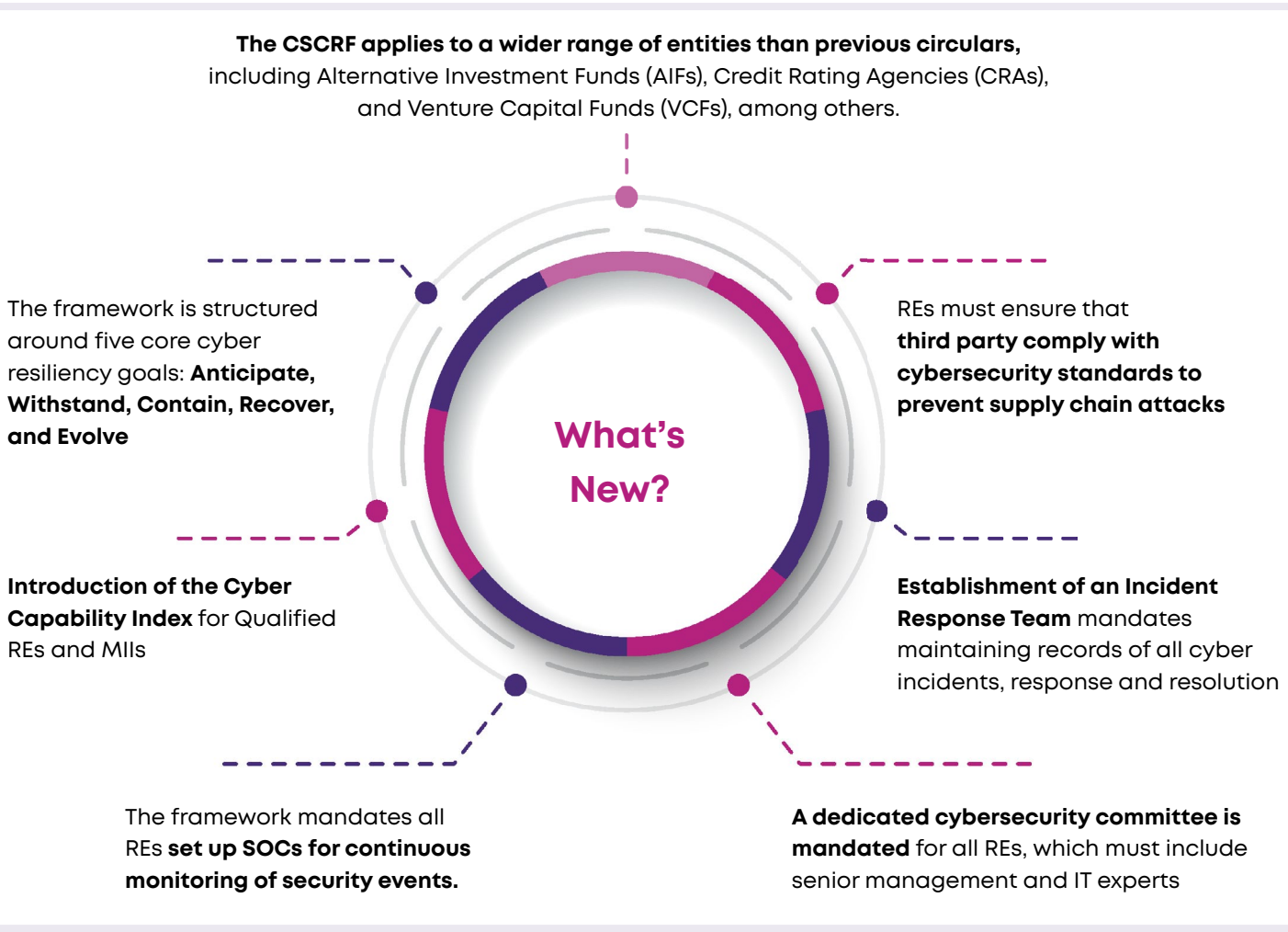
**Abhijit Varma**

*Partner, Global Head of Tech Consulting*
**Uniqus Consultech Inc.**

# What's New?



The Securities and Exchange Board of India (SEBI) has introduced the Cybersecurity and Cyber Resilience Framework (CSCRF) as a comprehensive update to its previous cybersecurity guidelines. This framework explicitly supersedes all prior SEBI cybersecurity circulars etc. to create a unified framework that addresses the evolving nature of cyber threats more effectively than previous iterations.



# Overview of SEBI CSCRF Circular



## Background

- Since 2015, the Securities and Exchange Board of India (SEBI) has issued Cybersecurity and Cyber resilience frameworks (CSCRF) and various advisories for Market Infrastructure Institutions (MIIs) and other Regulated Entities (REs).
- However, on **20 August 2024,** to strengthen cybersecurity measures across the Indian securities market and ensure adequate cyber resiliency against cybersecurity incidents/ attacks, SEBI formulated **the Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs.**

## Objective

- CSCRF's main objectives are to proactively strengthen REs' security postures and prepare their operations to withstand and recover from cyber incidents.

**Enhance Scope of current CSCRF**

**Uniformity of cybersecurity guidelines for all REs**

**Strengthen the mechanism to deal with cyber risks, threats, incidents, etc.**

# Overview of SEBI CSCRF Circular



## Applicability

**The CSCRF is applicable to the following regulated entities (REs):**

1. Alternative Investment Funds (AIFs)
2. Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)
3. Clearing Corporations
4. Collective Investment Schemes (CIS)
5. Credit Rating Agencies (CRAs)
6. Custodians
7. Debenture Trustees (DTs)
8. Depositories
9. Designated Depository Participants (DDPs)
10. Depository Participants through Depositories
11. Investment Advisors (IAs)/ Research Analysts (RAs)
12. KYC Registration Agencies (KRAs)
13. Merchant Bankers (MBs)
14. Mutual Funds (MFs)/ Asset Management Companies (AMCs)
15. Portfolio Managers
16. Registrar to an Issue and Share Transfer Agents (RTAs)
17. Stock-Brokers through Exchanges
18. Stock Exchanges
19. Venture Capital Funds (VCFs)

## Timeline for Implementation

**The CSCRF has been updated with new standards and controls, hence SEBI has provided a glide-path for adoption of the CSCRF.**

For six categories of REs, where cybersecurity and cyber resilience circular **already exists**

**1st January 2025**

**1st April 2025**

For other REs, where CSCRF is being **issued for the first time**

# CSCRF – The Framework



SEBI's CSCRF framework provides a standardized approach to implement various cybersecurity and cyber resilience methodologies, such as ISO 27000 series, CIS v8, NIST 800-53, etc. Below is the CSCRF framework structure that SEBI expects RE to implement for compliance.

| Cyber Resilience Goals | EVOLVE | | | | | |
|---|---|---|---|---|---|---|
| | ANTICIPATE | | | | WITHSTAND & CONTAIN | RECOVER |
| **Cyber Security Function** | **GOVERNANCE** | **IDENTIFY** | **PROTECT** | **DETECT** | **RESPOND** | **RECOVER** |
| **Objectives** | Establish & monitor the RE's cybersecurity risk management strategy, expectations, and policy with appropriate roles and responsibilities | RE's data personnel, devices, systems, and facilities are identified and managed as per organization's risk strategy | Safeguard to ensure RE's cyber resiliency are put in place to forestall compromises of missions/business function from adversary attacks | Identify and analyze possible cybersecurity attacks and compromises | Targeted actions, processes and procedures are executed with respect to a detected cybersecurity incident | Restore systems and services that were impacted by a cybersecurity incident |
| **Domains** | Organizational Context | Asset Management | Identity Management, Authentication, Access Control | Security Continuous Monitoring | Incident Management | Incident Recovery Plan Execution |
| | Roles, Responsibilities & Authorities | Risk Assessment | Awareness & Training | Detection Process | Incident Response Reporting and Communication | Incident Recovery Communication |
| | Policy | | Data Security | | Incident Analysis | Improvements |
| | Oversight | | Information Protection Processes and Procedures | | Improvements | |
| | Risk Management | | Maintenance | | | |
| | Cybersecurity Supply chain Risk Management | | | | | |

*Refer: Figure 1: CSCRF Overview (SEBI Circular)*

# CSCRF – Important Highlights



CSCRF highlights the importance of governance and supply chain risk Management, and at the same time, it focuses on evolving security guidelines such as data classification and localization, Application Programming Interface (API) security, Security Operations Centre (SOC), and measuring its efficacy, Software Bill of Materials (SBOM), etc.

1

### Security Operations Centre (SOC)

CSCRF mandates that all REs establish appropriate security monitoring mechanisms through a Security Operation Centre (SOC). The SOC can be onboarded through the RE's own/ group SOC, market SOC, or any other third-party managed SOC.

2

### Software Bill of Materials (SBOM)

REs to maintain a formal record containing the details and supply chain relationships of various components, such as open-source code, commercial components, etc., used in building software. The SBOM enumerates these components in a product.

3

### Data Classification & Localization

All the data generated (including creation and storage) within the legal boundaries of India remains within the legal boundaries of India. CSCRF has provided standards on Data Localization for:

- Regulatory Data
- IT and Cybersecurity Data

4

### VAPT after Major Change/ Major Release

CSCRF has mandated VAPT after every major release. Few example of major release(s)/ change(s):

- Implementation of a new SEBI circular.
- Changes in core versions of software
- Introduction of new security protocols

5

### Application Programming interface (API) security

Application Programming Interface (API) security and Endpoint security solutions shall be implemented with rate limiting, throttling, and proper authentication and authorization mechanisms.

6

### Cybersecurity and Quantum Computing

To mitigate the risk of Quantum Computing enabling breaking of the asymmetric cryptographic systems, REs have been provided guidelines, such as:

- Maintain inventory of cryptographic assets
- Explore the feasibility to adopt PQC and technologies like Quantum Key Distribution (QKD)

# CSCRF – Compliance Requirements



## Obligations of REs

Put in place appropriate systems and procedures to ensure compliance with the provisions (i.e., applicable standards and guidelines) of CSCRF.

**Conduct cyber audit** as per CSCRF and **submit audit reports to SEBI** along with other required documents as per timelines provided in the CSCRF.

For ease of compliance, REs must **comply with all applicable standards and mandatory guidelines** as mentioned in CSCRF.

MIIs and Qualified REs shall strive to build an automated tool and suitable dashboards (preferably integrated with a log aggregator) for submitting compliance with CSCRF.

# CSCRF – Compliance Requirements



CSCRF follows a graded approach and classifies the REs in five categories based on their span of operations and certain thresholds like number of clients, trade volume, asset under management, etc.

| Key CSCRF Compliance Requirements with Periodicity | Market Infrastructure Institutions (MIIs) | Qualified REs | Mid-size REs | Small-size REs | Self-certification REs |
|---|---|---|---|---|---|
| Cyber resilience third-party assessment using CCI<br>*Self-assessment for Qualified REs | ✓ (Half-Yearly) | ✓ (Annually) | | | |
| IT Committee for REs<br>1 external independent expert on cyber security | ✓ (Quarterly) | ✓ (Quarterly) | ✓ (Quarterly) | | |
| Functional Efficacy of SOC | ✓ (Half-Yearly) | ✓ (Half-Yearly) | ✓ (Annually) | ✓ (Annually) | ✓ (Annually) |
| Red Teaming exercise | ✓ (Half-Yearly) | ✓ (Half-Yearly) | | | |
| Threat hunting | ✓ (Quarterly) | ✓ (Quarterly) | | | |
| ISO 27001 Audit and Certification<br>Within 1 year of issuance of CSCRF | ✓ | ✓ | | | |
| VAPT | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cyber Audit | ✓ (Twice/ yr) | ✓ (Twice/ yr) | ✓ (Once/ yr) | ✓ (Once/ yr) | |

# Suggested Approach to CSCRF



## Identify

- Identify CSCRF requirements based on the RE category.
- **Identify stakeholders#** across the CSCRF value chain.
- **Conduct Table-Top exercises#** with stakeholders to identify high-level gaps against CSCRF requirements.
- Identify the **current state of security capabilities#.**

## Assess

- Conduct a detailed assessment against CSCRF standards and guidelines and identify gaps.
- Risk-prioritize mitigation actions and develop a roadmap in line with CSCRF compliance reporting timelines.

## Design

- Develop/update CSCRF policies, procedures, and templates in line with the standards, guidelines & reporting requirements of CSCRF.
- Identify, evaluate, and select solutions/ methods/ vendors/ updates, etc., to comply with CSCRF's requirements.

## Implement

- Implement the updated policies, procedures, templates, tools, solutions, etc.
- Monitor KPIs and iterate improvements to achieve adherence to CSCRF requirements.

## Report & Certify

- Conduct pre-certification assessments (including CCI) to assess readiness.
- ISO Certification (MIIs & Qualified REs).
- Identify & contract CERT-In empaneled auditor.
- Conduct Cyber Audit and submit audit reports to SEBI for certifying compliance.

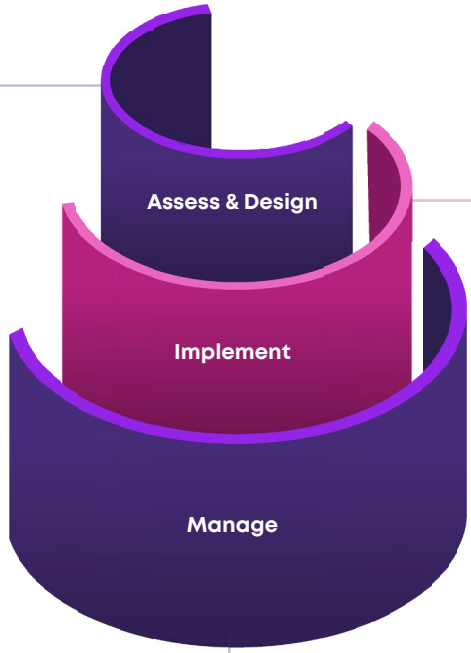
*#Refer "Immediate Actions"*

# How can Uniqus help?



We have developed a customized approach to help clients meet the CSCRF requirements based on their current state of maturity and mandatory requirements and incorporate the future needs of the organization based on its strategy and evolving threat landscape. We offer full spectrum Cyber services in a collaborative, alliance-led, fit-for-purpose, and business-centric model.

- CSCRF Current State Assessment with Risk-Prioritized Roadmap
- Technical Security Assessments – VA/ PT, API Security, Cloud Security, Red Teaming, Threat Hunting, SOC, etc.
- Cyber GRC Framework development including policies, procedures, plans, templates, etc.
- Design of Cyber Architecture, Tools/ Solutions specifications, Third-Party Risk Management, etc.



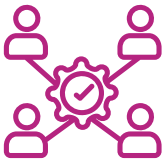

- Cyber Program Management Office (PMO) for Implementation
- Cyber Tools/ Solutions (SOC, Threat Intelligence, Data Classification, etc.) implementation with Alliance Partners
- Cyber GRC implementation
- Automation & Dashboarding for Continuous Controls/ Compliance Monitoring (CCM)

- Operate, Monitor & Manage Cyber GRC
- Cyber Capability Index (CCI) Maturity monitoring and improvement through Automation
- External Independent Expert on Cybersecurity for IT Committee
- Compliance Reporting Management

# Key Actions



We have defined some immediate key actions, which Uniqus can support the REs with to implement an optimal approach for SEBI's CSCRF.



**Identify key stakeholders & formulate CSCRF committee**

**Review current security posture, including third-party risk**

**Update existing policies and procedures aligned to CSCRF**

**Implement/ Enhance Threat Monitoring and Incident Reporting tools**

# A TEAM THAT
# YOU CAN TRUST TO DELIVER


**Jamil Khatri**
Co-Founder & CEO
jamilkhatri@uniqus.com

**Sandip Khetan**
Co-Founder & Global Head of ARC
sandip.khetan@uniqus.com

**Anu Chaudhary**
Partner, Global Head of ESG Consulting
anuchaudhary@uniqus.com

**Abhijit Varma**
Partner, Global Head of Tech Consulting
av@uniqus.com

**Bharat Chadha**
Partner, Tech Consulting
bharatchadha@uniqus.com

**Mitushi Pitti**
Partner, Tech Consulting
mitushipitti@uniqus.com

**Tarandeep Bindra**
Associate Partner, Tech Consulting
tarandeepbindra@uniqus.com

**Anupreet Kaur**
Director, Tech Consulting
anupreetkaur@uniqus.com

**Hammad Malik**
Director, Tech Consulting
hammadmalik@uniqus.com

**Janmin Shah**
Director, Tech Consulting
janminshah@uniqus.com

**Kunal Gandhi**
Director, Tech Consulting
kunalgandhi@uniqus.com


uniqus

**CHANGE THE WAY CONSULTING IS DONE**

To know more about us, please visit ***www.uniqus.com***