CSCRF – Our Point of View

Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs) from Securities Exchange Board of India (SEBI)

August 2024

kpmg.com/in

KPMG. Make the Difference.

Introduction

- The Securities and Exchange Board of India (SEBI) has announced a new Cybersecurity and Cyber Resilience Framework (CSCRF) on 20th August 2024 which aims to address cybersecurity challenges and enhance cyber resilience of SEBI regulated entities across the Indian financial markets.
- This new framework is to be implemented and be effective in a phased manner starting January 2025.
- SEBI regulated organisation are expected to deploy the framework as a robust and comprehensive approach towards their cybersecurity and resilience journey.

01 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)

02 CSCRF and its components

- The CSCRF is a comprehensive set of guidelines designed to enhance **both cybersecurity and cyber resilience** maturity of the entities regulated by SEBI.
- CSCRF is based on five cyber resiliency goals namely **Anticipate, Withstand, Contain, Recover and Evolve.**
- The cybersecurity approach covers various aspects from governance to operational controls **across Identify, Detect, Protect, Respond, and Recover** functions.

The cyber resiliency goals have been mapped to different cybersecurity functions:

	Cyber Resilience Goal: **Evolve**					
Cyber Resilience Goal	**Anticipate**				**Withstand and Contain**	**Recover**
Cybersecurity Function	Governance	Identify	Protect	Detect	Respond	Recover

The cybersecurity functions are to be implemented by REs through various cybersecurity controls. The controls are defined in the first two parts and are supported with compliance formats and templates in the next two parts:

Part 1: Objectives and Standards: The objectives highlight goals, which a security control needs to achieve.

Part 2: Guidelines: The guidelines recommend measures for complying with standards.

Part 3: Compliance Formats

Part 4: Annexures and References

03 Cyber Capability Index

- CSCRF has introduced a Cyber Capability Index (CCI).
- The CCI enables rating the cybersecurity and resilience controls of the REs and submit their CCI scores.
- The CCI index is calculated on the basis of 23 parameters. These parameters have been given corresponding target and different weightages in the index.

04 Key Obligations of REs

- REs shall put in place appropriate systems and procedures to ensure compliance with the provisions of CSCRF.
- Conduct cyber audits and submit compliance reports as per timelines provided in the CSCRF.
- Compliance reporting shall cover - Cyber resilience assessments, Cyber Capability Index reports, ISO Audit reports, VAPT reports, SOC effectiveness report, Cyber Audit reports.

05 Timelines for Report Submission

- There are timelines defined for REs in the circular based on the category that the RE falls under
- Evidence of compliance with the CSCRF including reports for ISO audit, VAPT assessments, Cyber audits, etc. shall have to be submitted as per the timelines defined.
- The timelines for reporting are based on the category of the REs and spread across Quarterly, Half-Yearly or Annually time periods.

06 Timeline for Implementation of CSCRF

For entities where cybersecurity and cyber resilience circular already exists
January 01, 2025

All other entities where CSCRF made applicable for the first time
April 01, 2025

07 Challenges of CSCRF

The CSCRF Framework supports REs to be cyber resilient. KPMG in India foresees a few hidden challenges that we can support REs in order to be compliant.

Board/ Partners/ Proprietors approvals for various activities

- Cybersecurity and cyber resilience policy
- Cyber crisis management plan
- List of critical systems
- CSCRF and VAPT reports

Data classification and localisation requirements

- Setting up robust security controls for data generated / managed / processed by REs, CSCRF classifies data in two categories: ‘Regulatory Data’ and ‘IT and Cybersecurity Data’.
- While ‘Regulatory Data’ is mandatorily localized, dispensation for ‘IT and Cybersecurity Data’ for offshoring has been given with suitable security controls.

Supply chain risk identification

- Designing and assessing cybersecurity supply chain risk management strategy/ process
- Creating SBOM’s (Software Bill of Material)

Application programming interface (API) security

- Performing API discovery, Access management, Rate Limiting, Zero-trust

Data protection measures

- Strong data protection measures (for both at-rest and in-transit data), with industry standard encryption algorithms, to be put in place

Response and recovery

- Develop, maintain and sustain comprehensive incident response plans and procedures
- Performing incident analysis and improvement

08 How Our Cyber Maturity Assessment (CMA) will help you:

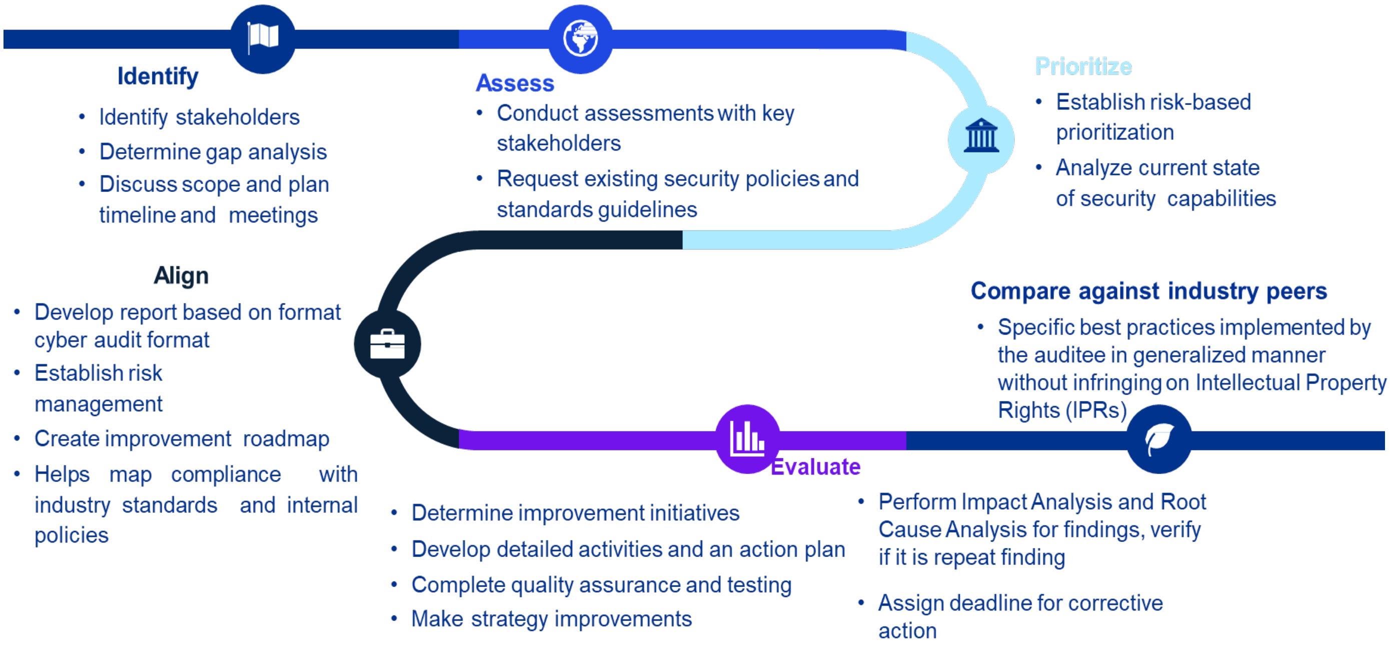
Our Cyber Maturity Assessment approach is beyond pure technical preparedness —taking a rounded view of people, process and technology. Our CMA framework encapsulates the SEBI CSCRF requirements. It provides a solution that not only supports your compliance needs but also gives you a possible answer to your cybersecurity posture.

Our Cyber Framework Characteristics

- Better coverage
- Flexible assessment
- Automated
- Comprehensive end-to-end solution

09 Roadmap to CSCRF compliance through our CMA

The CMA delivers an understanding of cyber maturity and any control gaps in an organisation's cybersecurity landscape to allow identification and prioritisation of remediation. This gives organisation the ability to demonstrate operational compliance.



Identify

- Identify stakeholders
- Determine gap analysis
- Discuss scope and plan timeline and meetings

Assess

- Conduct assessments with key stakeholders
- Request existing security policies and standards guidelines

Prioritize

- Establish risk-based prioritization
- Analyze current state of security capabilities

Align

- Develop report based on format cyber audit format
- Establish risk management
- Create improvement roadmap
- Helps map compliance with industry standards and internal policies

Compare against industry peers

- Specific best practices implemented by the auditee in generalized manner without infringing on Intellectual Property Rights (IPRs)

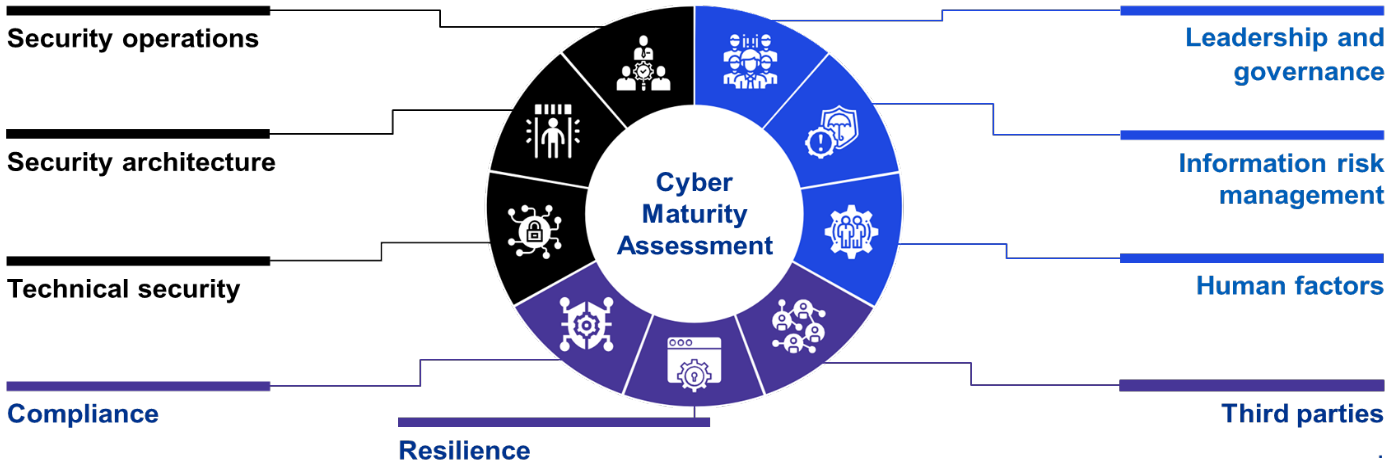
Evaluate

- Determine improvement initiatives
- Develop detailed activities and an action plan
- Complete quality assurance and testing
- Make strategy improvements

- Perform Impact Analysis and Root Cause Analysis for findings, verify if it is repeat finding
- Assign deadline for corrective action

10 Our Core Cyber Framework

KPMG in India has combined international information security standards with its leading global practices in cybersecurity to develop the **Core Cyber Framework**. The approach addresses nine critical functional areas that provide an extensive view of your organisation’s cyber maturity. The SEBI’s CSCRF requirements are encapsulated as a part of our comprehensive framework.



Cyber Maturity Assessment

- Security operations
- Security architecture
- Technical security
- Compliance
- Resilience
- Leadership and governance
- Information risk management
- Human factors
- Third parties

.

Why KPMG in India?

KPMG in India professionals will work with your team and conduct a combination of interviews, workshops, policy and process reviews and technical testing to help you manage your cybersecurity issues. To strategically enable your ongoing transformation, KPMG in India brings a combination of strengths across — cyber experience, deep business understanding and skilled people who deliver innovative thinking and practical implementation. We'll use our strengths to help you achieve compliance and improve maturity.

Global

Through our global network of member firms, there are over 270,000+ professionals in 143 countries and territories. KPMG in India cyber professionals have deep experience and provide a global multidisciplinary view of cyber risk, helping carry security throughout your organisation.

Distinctive

KPMG in India professionals bring a combination of vast technological experience, deep business and industry knowledge and creative professionals who are passionate about helping you protect and build stakeholder trust.

Our cyber agenda

KPMG in India aims to drive resolution for some of the world's leading organisation to work together to solve some of the biggest security challenges of today and tomorrow.

Committed to you

KPMG in India professional client relationships are built on mutual trust and long-term commitment to provide effective and efficient strategies.

List of Entities that needs to comply by January 01, 2025

- MII's - Stock Exchanges, Clearing Corporation and Depositories
- Stock Brokers / Depository Participants
- Mutual Funds / Asset Management Companies (AMCs)
- KYC Registration Agencies
- Qualified Registrars to an Issue / Share Transfer Agents (QRTAs)
- Portfolio Managers

KPMG in India contacts:

Atul Gupta
Partner and Head,
Digital Trust
T: +91 124 336 9001
E: atulgupta@kpmg.com

Nitin Shah
Partner and Head, Cyber Security
Strategy and Governance
T: ++91 124 336 9001
E: nitinshah@kpmg.com

Merril Cherian
Partner, Cyber Security
Strategy and Governance
T: +91 806 833 5000
E: mcherian@kpmg.com

Vipul Ubale
Associate Partner, Cyber
Security Strategy and
Governance
T: +91 226 134 9200
E: vipulubale@kpmg.com

Akanksha Saxena
Director, Cyber Security Strategy
and Governance
T: +91 124 336 9001
E: akankshasaxena@kpmg.com

kpmg.com/in

Access our latest insights
on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only. (033_BRO0824_AB)