भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 ***August 20, 2024***

प्रति

सभी आनुकल्पिक निवेश निधियाँ (एआईफ)
सभी निर्गमन बैंकर और स्व-प्रमाणित सिंडीकेट बैंक
सभी समाशोधन निगम (क्लीयरिंग कारपोरेशन)
सभी सामूहिक निवेश स्कीमें
सभी क्रेडिट रेटिंग एजेंसियाँ
सभी अभिरक्षक (कस्टोडियन)
सभी डिबेंचर न्यासी (ट्रस्टी)
सभी निक्षेपागार (डिपॉज़िटरी)
सभी अभिहित निक्षेपागार सहभागी (डीडीपी)
सभी निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) [निक्षेपागारों (डिपॉज़िटरी) के जरिए]
सभी निवेश सलाहकार / अनुसंधान विश्लेषक
सभी केवाईसी रजिस्ट्रीकरण एजेंसियाँ
सभी मर्चेंट बैंकर
सभी म्यूचुअल फंड / असेट मैनेजमेंट कंपनियाँ
सभी पोर्टफोलियो प्रबंधक
सभी निर्गम रजिस्ट्रार और शेयर अंतरण अभिकर्ता (आरटीए)
सभी स्टॉक दलाल (ब्रोकर) [एक्सचेंजों के जरिए]
सभी स्टॉक एक्सचेंज
सभी जोखिम पूँजी निधियाँ

To,

All Alternative Investment Funds (AIFs)
All Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)
All Clearing Corporations
All Collective Investment Schemes (CIS)
All Credit Rating Agencies (CRAs)
All Custodians
All Debenture Trustees (DTs)
All Depositories
All Designated Depository Participants (DDPs)
All Depository Participants through Depositories
All Investment Advisors (IAs) / Research Analysts (RAs)
All KYC Registration Agencies (KRAs)
All Merchant Bankers (MBs)
All Mutual Funds (MFs)/ Asset Management Companies (AMCs)
All Portfolio Managers
All Registrar to an Issue and Share Transfer Agents (RTAs)
All Stock Brokers through Exchanges
All Stock Exchanges
All Venture Capital Funds (VCFs)

महोदय / महोदया,

विषय : <u>सेबी से विनियमित (रेग्यूलेटेड) एंटिटियों के लिए साइबर सुरक्षा और साइबर हमलों से निपटने की क्षमता का ढाँचा (सीएससीआरएफ)</u>

पृष्ठभूमि:

1. सेबी ने वर्ष 2015 में बाजार की बुनियादी संस्थाओं (एमआईआई) के लिए साइबर सुरक्षा और साइबर हमलों से निपटने की क्षमता का ढाँचा निर्धारित किया था । उसके बाद, सेबी ने वर्ष 2015 के उस परिपत्र (सर्कुलर) की तर्ज पर नीचे बताई गई विनियमित (रेग्यूलेटेड) एंटिटियों के लिए भी साइबर सुरक्षा और साइबर हमलों से निपटने की क्षमता के संबंध में कुछ और प्रावधान निर्धारित किए थे :
   1.1 स्टॉक दलाल (ब्रोकर) और निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट)
   1.2 म्यूचुअल फंड / असेट मैनेजमेंट कंपनियाँ
   1.3 केवाईसी रजिस्ट्रीकरण एजेंसियाँ
   1.4 अर्हित निर्गम रजिस्ट्रार और शेयर अंतरण अभिकर्ता (क्यूआरटीए)
   1.5 पोर्टफोलियो प्रबंधक

2. इसके अलावा, सेबी ने साइबर सुरक्षा की बेहतरीन पद्धतियाँ अपनाने के संबंध में विनियमित (रेग्यूलेटेड) एंटिटियों को समय-समय पर कई एडवाइज़री भी जारी की हैं ।

3. भारत के प्रतिभूति बाजार (सिक्यूरिटीज मार्केट) में साइबर सुरक्षा की व्यवस्था को और मजबूत बनाने के लिए और यह सुनिश्चित करने के

Dear Sir / Madam,

Subject: <u>Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)</u>

Background:

1. SEBI had issued Cybersecurity and Cyber resilience framework for Market Infrastructure Institutions (MIIs) in 2015. Subsequently, SEBI had issued other Cybersecurity and Cyber resilience frameworks in line with MIIs circular of 2015 for following REs:
   1.1. Stock Brokers and Depository Participants
   1.2. Mutual Funds (MFs)/ Asset Management Companies (AMCs)
   1.3. KYC Registration Agencies (KRAs)
   1.4. Qualified Registrar to an Issue and Share Transfer Agents (QRTAs)
   1.5. Portfolio Managers

2. Further, SEBI has also issued various advisories to REs, from time to time, on Cybersecurity best practices.

3. In order to strengthen the cybersecurity measures in Indian securities market, and to ensure adequate cyber resiliency against

लिए कि साइबर हमलों आदि से निपटने की पर्याप्त व्यवस्था हो, सेबी से विनियमित (रेग्यूलेटेड) एंटिटियों के लिए साइबर सुरक्षा और साइबर हमलों से निपटने की क्षमता का ढाँचा (सीएससीआरएफ) इससे जुड़े सभी व्यक्तियों के परामर्श से निर्धारित किया गया है । सीएससीआरएफ का ढाँचा निर्धारित करने का उद्देश्य यह है कि साइबर हमलों से निपटने की क्षमता को और मजबूत बनाने के लिए तथा सेबी से विनियमित (रेग्यूलेटेड) एंटिटियों के यहाँ साइबर सुरक्षा की व्यवस्था को और मजबूत बनाने के लिए मानदंड और दिशानिर्देश निर्धारित किए जा सकें । इस तरह से इस संबंध में सेबी ने साइबर सुरक्षा के बारे में पहले से जो भी परिपत्र (सर्कुलर) / दिशानिर्देश / एडवाइज़री / पत्र जारी किए हुए हैं (जिनकी सूची **संलग्नक-1** में दी हुई है), उनकी जगह अब सीएससीआरएफ का यह ढाँचा ले लेगा ।

cybersecurity incidents/ attacks, Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs has been formulated in consultation with the stakeholders. The CSCRF aims to provide standards and guidelines for strengthening cyber resilience and maintaining robust cybersecurity of SEBI REs. This framework shall supersede existing SEBI cybersecurity circulars/ guidelines/ advisories/ letters (list of such superseded circulars/ guidelines/ advisories/ letters are given as part of the framework attached as **Annexure-1**).

उद्देश्य:

4. सीएससीआरएफ का ढाँचा निर्धारित करने का मुख्य उद्देश्य यह है कि नए-नए तरह के साइबर हमलों के खतरों से निपटा जा सके, साइबर सुरक्षा के क्षेत्र में अपनाए गए मानदंडों के अनुरूप इस ढाँचे में प्रावधान किए जा सकें, ऑडिट कारगर ढंग से किए जा सकें और सेबी से विनियमित (रेग्यूलेटेड) एंटिटियों के यहाँ इनका पूरा पालन सुनिश्चित हो सके । इस सीएससीआरएफ के ढाँचे में विनियमित (रेग्यूलेटेड) एंटिटियों के लिए रिपोर्टिंग के एक-जैसे फॉर्मेट भी निर्धारित कर दिए गए हैं ।

Objective:

4. The key objective of CSCRF is to address evolving cyber threats, to align with the industry standards, to encourage efficient audits, and to ensure compliance by SEBI REs. The CSCRF also sets out standards formats for reporting by REs.

क्या तरीका अपनाया जाएगा:

5. सीएससीआरएफ के तहत मानदंड निर्धारित किए गए हैं, और जिसमें साइबर हमलों से

Approach:

5. The CSCRF is standards based and broadly covers the five cyber resiliency goals adopted from Cyber Crisis

निपटने के लिए पाँच लक्ष्यों का जिक्र किया गया है, ताकि साइबर हमलों और साइबर आतंकवाद की घटनाओं से निपटा जा सके । ये पाँचों लक्ष्य सीईआरटी-इन के "साइबर क्राइसिस मैनेजमेंट प्लान" (सीसीएमपी) का हिस्सा हैं, जिनमें शामिल हैं:

5.1 तैयारी रखें
5.2 सामना करें
5.3 लगाम कसें
5.4 दुरुस्त करके बहाल करें
5.5 लगातार बेहतर बनते रहें

Management Plan (CCMP) of Indian Computer Emergency Response Team (CERT-In) for countering Cyber Attacks and Cyber Terrorism including:

5.1. Anticipate
5.2. Withstand
5.3. Contain
5.4. Recover
5.5. Evolve

6. साइबर सुरक्षा के इंतजाम इन्हीं लक्ष्यों के आधार पर किए गए हैं, यानि कि:

6.1 समूची व्यवस्था निर्धारित की जाती है
6.2 यह देखा जाता है कि क्या-क्या सिस्टम और व्यवस्थाएँ हैं
6.3 फिर उनकी सुरक्षा के इंतजाम किए जाते हैं
6.4 फिर साइबर हमलों की गुंजाइश का पता लगाया जाता है
6.5 फिर साइबर हमलों की घटनाओं पर कार्रवाई की जाती है
6.6 फिर अंत में सिस्टम, व्यवस्थाओं और सेवाओं को दुरुस्त करके बहाल किया जाता है

6. These cyber resiliency goals have been linked with the following cybersecurity functions:

6.1. Governance
6.2. Identify
6.3. Protect
6.4. Detect
6.5. Respond
6.6. Recover

7. इस ढाँचे के तहत पाँच तरह की विनियमित (रेग्यूलेटेड) एंटिटियों के लिए अलग-अलग पैमाने निर्धारित किए गए हैं, जो उनके कामकाज के दायरे के आधार पर और इन बातों के आधार पर निर्धारित किए गए हैं कि उनके ग्राहकों की संख्या कितनी है, उनके यहाँ ट्रेडिंग कितनी होती है, उनका ए.यू.एम. कितना है, आदि:

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

7.1 बाजार की बुनियादी संस्थाएँ (एमआईआई)
7.2 क्वालिफाइड विनियमित (रेग्यूलेटेड) एंटिटियाँ
7.3 मझौली विनियमित (रेग्यूलेटेड) एंटिटियाँ
7.4 छोटी विनियमित (रेग्यूलेटेड) एंटिटियाँ
7.5 स्व-प्रमाणित विनियमित (रेग्यूलेटेड) एंटिटियाँ

7.1. Market Infrastructure Institutions (MIIs)
7.2. Qualified Res
7.3. Mid-size REs
7.4. Small-size Res
7.5. Self-certification REs

8. इस ढाँचे में यह बताया गया है कि साइबर सुरक्षा के लिए और साइबर हमलों से निपटने की क्षमता को और मजबूत बनाने के लिए कैसे-कैसे और क्या-क्या व्यवस्था की जाए । इसे बेहतर ढंग से समझा जा सके तथा इसका पालन भी सहजता से किया जा सके, इसके लिए इस दस्तावेज को चार हिस्सों में बाँटा गया है:

8. The framework provides a structured methodology to implement various solutions for cybersecurity and cyber resiliency. In order to facilitate better understanding and ease of compliance, the document is divided into four parts:

8.1 भाग-I: उद्देश्य और मानदंड - इस हिस्से में परिभाषाएँ दी गई हैं; यह बताया गया है कि पालन कैसे-कैसे करना है; यह बताया गया है कि ऑडिट रिपोर्ट कब-कब प्रस्तुत करनी है; और इसके उद्देश्य बताए गए हैं तथा मानदंडों का जिक्र किया गया है ।

8.1. Part I: Objectives and Standards – It contains definitions, framework compliance matrix, audit report timelines, objectives and standards.

8.2 भाग-II: दिशानिर्देश - इस हिस्से में यह बताया गया है कि साइबर सुरक्षा के लिए और उसकी व्यवस्था के लिए कैसे-कैसे और क्या-क्या किया जा सकता है, और किस तरह से कुछ उद्देश्यों को पूरा किया जा सकता है तथा किस तरह से संबंधित मानदंडों को लागू किया जा सकता है । इनमें कुछ ऐसे दिशानिर्देश भी हैं, जिनका पालन करना लाज़िमी है और जिनके बारे में अलग से स्पष्ट कर दिया गया है ।

8.2. Part II: Guidelines – It contains guidelines which provide recommendations or suggestions on how to achieve a particular outcome or meet certain objectives and implement respective standards. There are certain guidelines, which are mandatory in nature and have been specified accordingly.

8.3 भाग-III: फॉर्मेट - इस हिस्से में वे फॉर्मेट दिए गए हैं, जिनमें यह रिपोर्ट दी जाएगी कि

8.3. Part III: Compliance Formats – It contains standard formats for the

सीएससीआरएफ के प्रावधानों का कितना पालन किया गया है ।

8.4 भाग-IV: अन्य - इस हिस्से में ऑडिटर के लिए दिशानिर्देश दिए गए हैं; यह बताया गया है कि अलग-अलग परिस्थितियों में साइबर हमलों से कैसे निपटा जाएगा; साइबर कैपेबिलिटी इंडेक्स (सीसीआई) के बारे में बताया गया है; सिक्यूरिटी ऑपरेशन्स सेंटर (एसओसी) की क्षमता के बारे में बताया गया है, आदि ।

9. जहाँ एक तरफ सीएससीआरएफ में यह बताया गया है कि समूची संचालन-व्यवस्था (सप्लाई चेन सहित) में जोखिमों को कम करना कितना जरूरी है, तो वहीं दूसरी तरफ इसमें इस बात पर भी जोर दिया गया है कि सुरक्षा के लिहाज से और किस-किस तरह के दिशानिर्देश निर्धारित किए जाने चाहिए जैसे कि डाटा क्लासिफिकेशन और डाटा लोकलाइजेशन की व्यवस्था, एप्लीकेशन प्रोग्रामिंग इंटरफेस (ए.पी.आई.) की सुरक्षा व्यवस्था, सिक्यूरिटी ऑपरेशन्स सेंटर की व्यवस्था (उसकी क्षमता के आकलन सहित), सॉफ्टवेयर बिल ऑफ मैटेरियल (एसबीओएम), आदि की व्यवस्था ।

10. सीएससीआरएफ का ढाँचा निर्धारित करने का उद्देश्य यह सुनिश्चित करना है कि छोटी विनियमित (रेग्यूलेटेड) एंटिटियों के यहाँ भी साइबर सुरक्षा के लिहाज से हर जरूरी कदम उठाए जाएँ और वे किसी भी तरह के साइबर हमले से निपटने में सक्षम हो सकें ।

11. एमआईआई और क्वालिफाइड विनियमित (रेग्यूलेटेड) एंटिटियों के लिए बनाए गए साइबर कैपेबिलिटी इंडेक्स (सीसीआई) की वजह से समय-समय पर यह पता चलता रहेगा कि उनके यहाँ साइबर हमलों से

submission of CSCRF compliance reports.

8.4. Part IV: Annexures and References - It contains guidelines to auditors, scenario-based cyber resilience testing, Cyber Capability Index (CCI), functional efficacy of Security Operations Centre (SOC), etc.

9. 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.

10. CSCRF aims to ensure that even smaller REs are equipped with adequate cybersecurity measures and achieve resiliency against cybersecurity incidents/ attacks.

11. Cyber Capability Index (CCI) for MIIs and Qualified REs shall help these REs to monitor and assess their progress and cyber resilience on a periodic basis.

निपटने की तैयारी कितनी है और वे इसमें अपनी कितनी पकड़ बना चुकी हैं ।

12. सीएससीआरएफ में यह बताया गया है कि सभी विनियमित (रेग्यूलेटेड) एंटिटियों को सिक्यूरिटी ऑपरेशन्स सेंटर (एसओसी) के जरिए सुरक्षा व्यवस्था करके कड़ी नज़र रखनी होगी । एसओसी की व्यवस्था विनियमित (रेग्यूलेटेड) एंटिटियाँ या तो अपने स्तर पर कर सकती हैं या ग्रुप स्तर पर कर सकती हैं या फिर उसके लिए मार्केट स्तर पर बने एसओसी का इस्तेमाल कर सकती हैं और या फिर किसी दूसरी एजेंसी आदि के एसओसी का इस्तेमाल कर सकती हैं, ताकि किसी भी तरह के साइबर हमले का पहले ही पता चल सके और तदनुसार कड़ी सुरक्षा व्यवस्था हो सके ।

12. CSCRF mandates that all REs are required to establish appropriate security monitoring mechanisms through Security Operation Centre (SOC). The onboarding of SOC can be done through RE's own/ group SOC or Market SOC or any other third-party managed SOC for continuous monitoring of security events and timely detection of anomalous activities.

13. ऐसा भी हो सकता है कि छोटी विनियमित (रेग्यूलेटेड) एंटिटियों को साइबर सुरक्षा के मामलों में पूरी जानकारी न हो और यदि उन्हें खुद का एसओसी बनाना पड़े तो उन पर खर्च का भी ज्यादा बोझ पड़ जाए, और इसी वजह से उनके लिए साइबर सुरक्षा से संबंधित दिशानिर्देशों का पालन करना मुश्किल हो जाए । इसी बात को ध्यान में रखते हुए, सीएससीआरएफ में एनएसई और बीएसई के लिए यह अनिवार्य कर दिया गया है कि वे मार्केट स्तर पर एक एसओसी (एम-एसओसी) की व्यवस्था करें, ताकि इस तरह की विनियमित (रेग्यूलेटेड) एंटिटियाँ भी साइबर सुरक्षा के इंतज़ामों से अछूती न रहें।

13. As compliance with the cybersecurity guidelines may be onerous for smaller REs due to the lack of knowledge and expertise in cybersecurity and the cost factor involved in setting up own SOC. Therefore, CSCRF mandates NSE and BSE to set up Market SOC (M-SOC) with the objective of providing cybersecurity solutions to such categories of REs.

14. सीएससीआरएफ में सभी बातें साफ कर दी गई हैं कि किस तरह की आईटी सेवाओं, किस तरह के *सॉफ्टवेयर एज़ ए सर्विस* (एसएएएस) सॉल्यूशन, किस तरह की *होस्ट*

14. CSCRF contains provisions with respect to various areas such as requirements of IT services, Software as a Service (SaaS) solutions, hosted

सर्विसेज़, डाटा क्लासिफिकेशन की व्यवस्था करनी होगी, और साथ ही यह भी बताया गया है कि विनियमित (रेग्यूलेटेड) एंटिटियाँ जो सॉफ्टवेयर सॉल्यूशन / एप्लीकेशन / प्रोडक्ट इस्तेमाल कर रही हों उनका उन्हें ऑडिट करवाना होगा ।

services, classification of data, audit for software solutions/ applications/ products used by REs, etc.

15. इस ढाँचे के प्रावधानों का कितना पालन हो रहा है, इसकी जानकारी देने की व्यवस्था भी सहज हो, इसके लिए रिपोर्टों के भी एक-जैसे फॉर्मेट निर्धारित कर दिए गए हैं ।

15. In order to simplify and streamline the reporting of compliance, structured formats for reports and submissions have been provided in the CSCRF.

इन पर लागू होगा:

16.यह ढाँचा नीचे बताई हुई विनियमित (रेग्यूलेटेड) एंटिटियों पर लागू होगा:

16.1 आनुकल्पिक निवेश निधियाँ (एआईफ)

16.2 निर्गमन बैंकर और स्व-प्रमाणित सिंडीकेट बैंक

16.3 समाशोधन निगम (क्लीयरिंग कारपोरेशन)

16.4 सामूहिक निवेश स्कीमें

16.5 क्रेडिट रेटिंग एजेंसियाँ

16.6 अभिरक्षक (कस्टोडियन)

16.7 डिबेंचर न्यासी (ट्रस्टी)

16.8 निक्षेपागार (डिपॉज़िटरी)

16.9 अभिहित निक्षेपागार सहभागी (डीडीपी)

16.10 निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) [निक्षेपागारों (डिपॉज़िटरी) के जरिए]

16.11 निवेश सलाहकार / अनुसंधान विश्लेषक

16.12 केवाईसी रजिस्ट्रीकरण एजेंसियाँ

16.13 मर्चेंट बैंकर

Applicability:

16. The framework shall be applicable to the following REs:

16.1. Alternative Investment Funds (AIFs)
16.2. Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)
16.3. Clearing Corporations
16.4. Collective Investment Schemes (CIS)
16.5. Credit Rating Agencies (CRAs)
16.6. Custodians
16.7. Debenture Trustees (DTs)
16.8. Depositories
16.9. Designated Depository Participants (DDPs)
16.10. Depository Participants through Depositories
16.11. Investment Advisors (IAs)/ Research Analysts (RAs)
16.12. KYC Registration Agencies (KRAs)
16.13. Merchant Bankers (MBs)

16.14 म्यूचुअल फंड / असेट मैनेजमेंट कंपनियाँ
16.15 पोर्टफोलियो प्रबंधक
16.16 निर्गम रजिस्ट्रार और शेयर अंतरण अभिकर्ता (आरटीए)
16.17 स्टॉक दलाल (ब्रोकर) [एक्सचेंजों के जरिए]
16.18 स्टॉक एक्सचेंज
16.19 जोखिम पूँजी निधियाँ

16.14. Mutual Funds (MFs)/ Asset Management Companies (AMCs)
16.15. Portfolio Managers
16.16. Registrar to an Issue and Share Transfer Agents (RTAs)
16.17. Stock Brokers through Exchanges
16.18. Stock Exchanges
16.19. Venture Capital Funds (VCFs)

कब से लागू होगा:

17. चूँकि सीएससीआरएफ में नए मानदंड आदि जोड़े गए हैं, इसलिए सीएससीआरएफ के प्रावधान कब से लागू होंगे, यह नीचे बताया गया है:

17.1 उन छह श्रेणियों की विनियमित (रेग्यूलेटेड) एंटिटियों के मामले में 1 जनवरी, 2025 से लागू होंगे, जिनके मामले में साइबर सुरक्षा और साइबर हमलों से निपटने की क्षमता के विषय से संबंधित परिपत्र (सर्कुलर) पहले ही जारी किया जा चुका है।

17.2 दूसरी विनियमित (रेग्यूलेटेड) एंटिटियों के मामले में 1 अप्रैल, 2025 से लागू होंगे, जिनके मामले में सीएससीआरएफ पहली बार लाया जा रहा है ।

18. विनियमित (रेग्यूलेटेड) एंटिटियों को अपने यहाँ उपयुक्त व्यवस्थाएँ और प्रक्रियाएँ निर्धारित करनी होंगी, ताकि सीएससीआरएफ के प्रावधानों (यानि कि लागू मानदंडों और दिशानिर्देशों) का पालन सुनिश्चित हो सके, और साथ ही वे उपरोक्त तारीखों के बाद सीएससीआरफ के अनुसार साइबर ऑडिट भी करवाएंगी । साइबर ऑडिट की रिपोर्टें (दूसरे जरूरी दस्तावेजों के साथ) सीएससीआरएफ

Implementation Period:

17. Since new standards and controls have been added in CSCRF, a glide-path for adoption of CSCRF provisions has been provided as under:

17.1. For six categories of REs where cybersecurity and cyber resilience circular already exists – by January 01, 2025.

17.2. For other REs where CSCRF is being issued for the first time – by April 01, 2025.

18. REs shall put in place appropriate systems and procedures to ensure compliance with the provisions (i.e., applicable standards and guidelines) of CSCRF, and conduct cyber audit as per CSCRF after the above-mentioned timelines. Cyber audit reports along with other required documents shall be submitted as per timelines provided in the CSCRF.

में बताई गई समय-सीमाओं के अनुसार प्रस्तुत करनी होंगी ।

19. सीसीसीआरएफ के प्रावधानों का पालन किए जाने की जानकारी उसी तरह दी जाएगी, जिस तरह से पहले से साइबर सुरक्षा के ऑडिट के सिलसिले में दी जाती है ।

19. The reporting of compliance with respect to CSCRF shall be done to the authority as per the existing mechanism of reporting for cybersecurity audit.

20. इस संबंध में विस्तृत ढाँचा इस परिपत्र के **संलग्नक-1** में दिया हुआ है ।

20. The detailed framework is enclosed at **Annexure-1** of this circular.

21. यह परिपत्र (सर्कुलर) भारतीय प्रतिभूति और विनिमय बोर्ड अधिनियम, 1992 (सेबी एक्ट, 1992) की धारा 11(1) [जो प्रतिभूति बाजार (सिक्यूरिटीज मार्केट) में निवेश करने वाले निवेशकों के हितों का संरक्षण करने और प्रतिभूति बाजार (सिक्यूरिटीज मार्केट) के विकास को बढ़ावा देने और उसे विनियमित (रेग्यूलेट) करने से संबंधित है] के तहत प्रदान की गई शक्तियों का प्रयोग करते हुए जारी किया जा रहा है ।

21. This circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

22. यह परिपत्र सक्षम प्राधिकारी की मंजूरी से जारी किया जा रहा है ।

22. The circular is issued with the approval of Competent Authority.

23. यह परिपत्र सेबी की वेबसाइट (www.sebi.gov.in) पर इन शीर्षकों के अंतर्गत दिया हुआ है: “कानूनी ढाँचा - परिपत्र”।

23. This circular is available on SEBI website at www.sebi.gov.in under the category “Legal” and drop “Circulars”.

भवदीय Yours Faithfully,

श्वेता बनर्जी Shweta Banerjee

उप महाप्रबंधक Deputy General Manager

दूरभाष / Phone: 022-26449509

ईमेल / Email: shwetas@sebi.gov.in

Annexure-1

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

Version 1.0

Date: August 20, 2024

Securities and Exchange Board of India

Plot no. C4-A, G Block, Bandra Kurla Complex,

Bandra (East), Mumbai – 400051, India

Tel.: +91-22-26449000/40459000

Website: www.sebi.gov.in

This page intentionally left blank

Executive Summary

The Information Technology Act, 2000 defines Cybersecurity as *"Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction".*

Technology has been a driving force in shaping the securities market, enabling greater efficiency, accessibility, and affordability. However, with swift technological advancements, protection of IT infrastructure and data has become a key concern for SEBI and its Regulated Entities (REs). Since 2015, SEBI has issued various cybersecurity and cyber resilience frameworks to address cybersecurity risks and enhance cyber resilience of SEBI REs. Further, SEBI has also issued several advisories on cybersecurity best practices for REs from time to time.

In order to enhance the scope of the current cybersecurity and cyber resilience framework, to ensure the need for uniformity of cybersecurity guidelines for all REs and to strengthen the mechanism to deal with cyber risks, threats, incidents, etc., the Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI REs has been formulated. CSCRF is a result of coordinated efforts after an extensive consultations and discussions with the stakeholders including Market Infrastructure Institutions (MIIs), REs, industry associations, government organizations (for example Indian Computer Emergency Response Team - CERT-In, National Critical Information Infrastructure Protection Centre, etc.), Industry Standard Forum (ISF), information security auditors, industry experts, Cloud Service Providers (CSPs), etc., and has also been reviewed by SEBI's High Powered Steering Committee on Cybersecurity (HPSC-CS).

The framework provides a standardized approach to implement various cybersecurity and cyber resilience methodologies. Standards such as ISO 27000 series, CIS v8, NIST 800-53, BIS Financial Stability Institute, CPMI-IOSCO guidelines, etc. were referred to while formulating this framework.

The framework follows a graded approach and classifies the REs in the following five categories based on their span of operations and certain thresholds[1] like number of clients, trade volume, asset under management, etc.:

i. Market Infrastructure Institutions (MIIs)
ii. Qualified REs
iii. Mid-size REs
iv. Small-size REs
v. Self-certification REs

[1] Refer 'Thresholds for REs' categorization' section

The framework is divided into four parts:

i. *Part I: Objectives and Standards*: The objectives highlight goals which a security control needs to achieve. The standards represent established principles for compliance with CSCRF.
ii. *Part II: Guidelines*: The guidelines recommend measures for complying with standards mentioned in this document. However, few of the guidelines are mandatory in nature and shall be complied by REs as applicable.
iii. Part III: Structured formats for compliance
iv. Part IV: Annexures and References

For ease of compliance, REs are required to comply with the all applicable standards and mandatory guidelines as mentioned in CSCRF.

The Structure of CSCRF

The framework is broadly based on two approaches: cybersecurity and cyber resilience. Cybersecurity approach covers various aspects from governance measures to operational controls and the cyber resilience goals include Anticipate, Withstand, Contain, Recover, and Evolve.

The framework also specifies guidelines to ensure standards are implemented in a uniform manner.

The summary of the CSCRF is as follows:

i. **Cyber Resilience Goal: Anticipate | Cybersecurity function: Governance**
   a. REs shall establish, communicate and enforce cybersecurity risk management roles, responsibilities, and authorities to foster accountability and continuous improvement.
   b. A comprehensive cybersecurity and cyber resilience policy shall be documented and implemented with the approval of the Board/ Partners/ Proprietor.
   c. CSCRF mandates MIIs, Qualified REs, and mid-size REs to prepare cyber risk management framework for identification and analysis, evaluation, prioritization, response and monitoring the cyber risks on a continuous basis.
   d. Cyber Capability Index (CCI): This shall be applicable only to MIIs and Qualified REs. MIIs shall conduct third-party assessment of their cyber resilience using CCI on a half-yearly basis. Qualified REs shall do self-assessment of their cyber resilience using CCI on a yearly basis.
   e. REs shall be solely accountable for all aspects related to third-party services including (but not limited to) confidentiality, integrity, availability, non-repudiation, security of their data and logs, and ensuring compliance with laws, regulations, circulars, etc. issued by SEBI/ Government of India. Accordingly, REs shall be responsible and accountable for any violations of the same.

ii. **Cyber Resilience Goal: Anticipate | Cybersecurity function: Identify**

a. REs shall identify and classify *critical systems* based on their sensitivity and criticality for business operations, services and data management. The Board/ Partners/ Proprietor of the RE shall approve the list of *critical systems*.

b. Risk assessment (including post-quantum risks[2]) of RE's IT environment shall be done on a periodic basis. Risk assessment shall include comprehensive scenario-based testing for assessing risks (including both internal and external risks) related to cybersecurity in REs' IT environment.

c. Threats, vulnerabilities, likelihoods, and impacts shall be used to understand inherent risks and undertake risk response prioritization.

iii. **Cyber Resilience Goal: Anticipate | Cybersecurity function: Protect**

a. Authentication and access policy along with effective log collection[3] and retention policy shall be documented and implemented.

b. REs shall design and implement network segmentation techniques to restrict access to the sensitive information, hosts, and services.

c. Layering of Full-disk Encryption (FDE) along with File-based Encryption (FE) shall be used for data protection.

d. There shall be separate production and non-production environments for the development of all software/ applications for critical systems and further feature enhancements.

e. Periodic audits shall be conducted by a CERT-In empanelled IS auditing organization to audit the implementation and provide compliance with the applicable standards and mandatory guidelines mentioned in the CSCRF.

f. Vulnerability Assessment and Penetration Testing (VAPT) shall be done to detect vulnerabilities in the IT environment for all *critical systems*, infrastructure components and other IT systems as defined in the framework. To undertake this activity, a comprehensive VAPT scope has also been specified.

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

h. ISO 27001 certification: ISO 27001 certification shall be mandatory for MIIs and Qualified REs as it provides essential security standards with respect to Information Security Management System (ISMS).

[2] Quantum computing is a rapidly emerging technology that exploits quantum mechanics' laws to solve complex problems. Post-quantum cryptography solutions can avert post-quantum risks and provide protection against quantum attacks.

[3] With all relevant fields including verbosity and relevancy.

iv. **Cyber Resilience Goal: Anticipate | Cybersecurity function: Detect**

a. REs shall establish appropriate security mechanisms through Security Operations Centre (SOC) [RE's own/ group SOC, third-party SOC, or market SOC] for continuous monitoring of security events and timely detection of anomalous activities.

b. Bombay Stock Exchange (BSE) and National Stock Exchange (NSE) have been mandated to setup Market SOC. Further, small-size REs and Self-certification REs have been mandated to be onboarded on the Market SOC.

c. MIIs and Qualified REs shall measure functional efficacy of their SOC on a half-yearly basis. Rest of the REs shall obtain functional efficacy of the SOC utilized by them on a yearly basis from the SOC service providers. A quantifiable method and an indicative list of parameters for measuring SOC efficacy has been given in this framework. The report of functional efficacy of Market SOC shall be provided by BSE and NSE to SEBI on a periodic basis.

d. Red Teaming: MIIs and Qualified REs shall conduct red teaming exercises as part of their cybersecurity framework.

v. **Cyber Resilience Goal: Withstand & Contain | Cybersecurity function: Respond**

a. All cybersecurity incidents shall be reported in a timely manner through the SEBI incident reporting portal.

b. All REs shall establish a comprehensive Incident Response Management plan and the corresponding SOPs.

c. All REs shall formulate an up-to-date Cyber Crisis Management Plan (CCMP).

d. In the event of an incident, Root Cause Analysis (RCA) shall be conducted to identify the cause(s) leading to the incident.

e. Where RCA is inconclusive, a forensic analysis shall be undertaken for detailed investigation of the cybersecurity incident.

vi. **Cyber Resilience Goal: Recover | Cybersecurity function: Recover**

a. A comprehensive response and recovery plan shall be documented. The plan shall be triggered to ensure prompt restoration of systems affected by the cybersecurity incident. An indicative recovery plan has been provided in the CSCRF.

b. Actions taken during recovery process shall be informed to all the relevant stakeholders as required.

vii. **Cyber Resilience Goal: Evolve**

Adaptive and evolving controls to tackle identified vulnerabilities and to reduce attack surfaces shall be created and incorporated into the RE's cybersecurity and cyber resilience strategy.

viii. **Compliance requirements**

The compliance reporting for CSCRF shall be done by the REs to their respective authorities[4] in the standardized formats mentioned in this framework as per the stated periodicity. A glide-path has been given to REs to comply with the CSCRF standards and mandatory guidelines. Since new standards and controls have been added in CSCRF, a glide-path for adoption of CSCRF provisions has been provided as under:

a. For six categories of REs where cybersecurity and cyber resilience circular already exists – by January 01, 2025.
b. For other REs where CSCRF is being issued for the first time – by April 01, 2025.

Further, to ensure the uniformity in auditing REs w.r.t. CSCRF, an auditors' checklist and guidelines has been included in this framework.

Future proofing of CSCRF

It is envisaged that quantum computing may be a reality in near future and it may be able to break the encryption schemes widely used today. Thus, quantum computing may evolve into one of the biggest cybersecurity threats and it may potentially expose financial systems to cyber-attacks. While it is still uncertain when quantum technology would be adopted on a large scale, its potential as a cyber threat to the securities market ecosystem is already a matter of concern. The CSCRF has provisions to address 'harvest now - decrypt later' attacks through continuous risk assessment and adoption of robust data protection measures.

The framework will continue to be updated based on the maturity of the technologies and their adoption by the REs to meet the future cybersecurity needs of securities market.

--o--

[4] Refer 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Table of Contents

Abbreviations

SN.	Abbreviation	Explanation/ Expansion
1.	ACL	Access Control List
2.	AIF	Alternative Investment Fund
3.	AMC	Asset Management Company
4.	API	Application Programming Interface
5.	ASVS	Application Security Verification Standard
6.	AUC	Asset Under Custody
7.	AUM	Asset Under Management
8.	BAS	Breach and Attack Simulation
9.	BASL	BSE Administration and Supervision Limited
10.	BOLT	BSE's on-line Trading System
11.	BSE	Bombay Stock Exchange
12.	BYOD	Bring Your Own Device
13.	C&C	Command and Control
14.	CART	Continuous Automated Red Teaming
15.	CCI	Cyber Capability Index
16.	CCMP	Cyber Crisis Management Plan
17.	CEH	Certified Ethical Hacker
18.	CEO	Chief Executive Officer
19.	CERT-In	Indian Computer Emergency Response Team
20.	CII	Critical Information Infrastructure
21.	CIO	Chief Information Officer
22.	CIS	Center for Internet Security
23.	CISM	Certified Information Security Manager
24.	CISO	Chief Information Security Officer

25.	COTS	Commercial Off The Shelf
26.	CSCRF	Cybersecurity and Cyber Resilience Framework
27.	CSIRT-Fin	Computer Security Incident Response Team – Finance sector
28.	CSK	Cyber Swachhta Kendra
29.	CSP	Cloud Service Provider
30.	CTCL	Computer to Computer Link
31.	CTI	Cyber Threat Intelligence
32.	CTO	Chief Technology Officer
33.	CVE	Common Vulnerabilities and Exposures
34.	CWE	Common Weakness Enumeration
35.	DB	Database
36.	DC	Domain Controller
37.	DDoS	Distributed Denial-of-Service
38.	DEV	Development
39.	DKIM	Domain Keys Identified Mail
40.	DLP	Data Loss Prevention
41.	DMARC	Domain-based Message Authentication Reporting & Conformance
42.	DNS	Domain Name System
43.	DR	Disaster Recovery
44.	EDR	Endpoint Detection and Response
45.	EPP	Endpoint Protection Platforms
46.	EPSS	Exploit Prediction Scoring System
47.	FDE	Full-disk Encryption
48.	FPO	Follow-on Public Offer

49.	FSB	Financial Stability Board
50.	HPSC-CS	High Powered Steering Committee on Cyber Security
51.	GoI	Government of India
52.	IaaS	Infrastructure as a Service
53.	IBT	Internet Based Trading
54.	IDS	Intrusion Detection System
55.	IOAs	Indicators of Attack
56.	IOCs	Indicators of Compromise
57.	IOSCO	International Organization of Securities Commissions
58.	IP	Internet Protocol
59.	IPO	Initial Public Offer
60.	IPS	Intrusion Prevention System
61.	IS	Information Security
62.	ISACA	Information Systems Audit and Control Association
63.	ISMS	Information Security Management System
64.	ISO	International Organization for Standardization
65.	IT	Information Technology
66.	KRA	KYC (Know Your Client) Registration Agency
67.	MASVS	Mobile Application Security Verification Standard
68.	MD	Managing Director
69.	MeitY	Ministry of Electronic and Information Technology
70.	MFA	Multi-Factor Authentication
71.	MII	Market Infrastructure Institution
72.	MTTC	Mean Time to Contain
73.	MTTD	Mean Time to Detect

74.	MTTR	Mean Time to Respond
75.	NCIIPC	National Critical Information Infrastructure Protection Centre
76.	NDR	Near Disaster Recovery
77.	NEAT	National Exchange for Automated Trading
78.	NIST	National Institute of Standards and Technology
79.	NSE	National Stock Exchange
80.	OS	Operating System
81.	OT	Operational Technology
82.	OTP	One Time Password
83.	OWASP	Open Web Application Security Project
84.	PaaS	Platform as a Service
85.	PDC	Primary Data Centre
86.	PII	Personal Identifiable Information
87.	PIM	Privileged Identity Management
88.	POLP	Principle of Least Privilege
89.	PQC	Post Quantum Cryptography
90.	QA	Quality Assurance
91.	QKD	Quantum Key Distribution
92.	QRTA	Qualified Registrar to an Issue and Share Transfer Agent
93.	RAT	Remote Access Trojan
94.	RBA	Risk Based Authentication
95.	RBI	Reserve Bank of India
96.	RCA	Root Cause Analysis
97.	RDP	Remote Desktop Protocol

98.	RE	Regulated Entity[5]
99.	RPO	Recovery Point Objective
100.	RTO	Recovery Time Objective
101.	SaaS	Software as a Service
102.	SANS	SysAdmin, Audit, Network and Security
103.	SBOM	Software Bill of Materials
104.	SCOT	Standing Committee on Technology
105.	SIEM	Security Information and Event Management
106.	SIT	System Integration Test
107.	SLA	Service Level Agreement
108.	SMB	Server Message Block
109.	SME	Small and Medium Enterprises
110.	SOAR	Security Orchestration, Automation, and Response
111.	SOC	Security Operations Centre
112.	SOP	Standard Operating Procedure
113.	SPF	Sender Policy Framework
114.	SSDLC	Secure Software Development Life Cycle
115.	SSVC	Stakeholder-Specific Vulnerability Categorization
116.	STQC	Standardisation Testing and Quality Certification
117.	TLP	Traffic Light Protocol
118.	UAT	User Acceptance Test
119.	UCC	Unique Client Code
120.	UEBA	User Entity and Behavior Analytics
121.	URL	Uniform Resource Locator

[5] Entities within SEBI's purview, refer to Securities Contracts (Regulation) Act 1956, SEBI Act 1992, and Depositories Act 1996.

122.	VAPT	Vulnerability Assessment & Penetration Testing
123.	VBA	Visual Basic for Application
124.	VPN	Virtual Private Network
125.	WAF	Web Application Firewall
126.	XDR	Extended Detection and Response

Definitions

1. **CIA triad[6]:**
   a. **Confidentiality:** Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.
   b. **Integrity:** Property of accuracy and completeness.
   c. **Availability:** Property of being accessible and usable on demand by an authorised entity.

2. **Critical Systems –**
   Entities shall identify and classify their critical IT systems. Following systems shall be included in critical systems (both on premise and cloud):
   a. Any system, if compromised, that will have an adverse impact on core and critical business operations.
   b. Stores/ transmits data as per regulatory requirements.
   c. Devices/ network through which critical systems are connected (through trusted channels).
   d. Internet facing applications/ systems.
   e. Client facing application/ systems.
   f. All the ancillary systems used for accessing/ communicating with critical systems either for operations or for maintenance.

3. **Cyber Capability Index (CCI) –**
   CCI is an index applicable for MIIs and Qualified REs which is calculated based on certain parameters as specified in this framework. The purpose of CCI is to ascertain the cyber resilience capabilities of MIIs and Qualified REs and their maturity in terms of implementation of cybersecurity measures.

4. **Cyber Event –**
   Any observable occurrence in an information system. Cyber events sometimes provide indication that a cybersecurity incident is occurring. – *FSB Cyber Lexicon*[7]

5. **Cyber Resilience –**
   The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents. – *FSB Cyber Lexicon*[8]

[6] https://www.fsb.org/wp-content/uploads/P130423-3.pdf
[7] https://www.fsb.org/wp-content/uploads/P130423-3.pdf
[8] https://www.fsb.org/wp-content/uploads/P130423-3.pdf

6. **Cyber Threat –**
   A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity. – *FSB Cyber Lexicon*[9]

7. **Cybersecurity Incident (Incident)–**
   Any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes in data, information without authorisation. – *CERT-In Cybersecurity directions*[10]

8. **Hosted Service -**
   Any IT/ SaaS provider rendering IT services/ SaaS solutions hosted on IT infrastructure either owned or controlled and managed by the service provider shall be broadly construed as hosted services. Hosted services have to fulfil the following technical specifications:
   1. Data center that hosts IT services/ SaaS solutions shall be ANSI/ TIA-942 rated-4 standard certified or equivalent (e.g. Tier 4) with complete fault tolerance and redundancy for every component.
   2. IT infrastructure shall atleast be of equivalent standard of MeitY Empanelment of Cloud Service offerings of Cloud Service Providers (CSPs) and audited by a STQC empanelled cloud audit organisation or equivalent established international agency.
   3. Summary of VAPT reports shall be made available to the REs and to the SEBI on demand.
   4. If the data center is operated from outside the legal boundaries of India, then a copy of REs' data in human/ application readable form shall be maintained within the legal boundaries of India.
   5. Hosted service provider shall ensure that there is no "*Kill Switch*" available in the Application, which would remotely disable the functioning of the solution.
   6. There shall be an explicit and unambiguous delineation/ demarcation of responsibilities with respect to all activities (including but not limited to technical, managerial, governance related, etc.) of the hosted services between the RE and Hosted service provider. The aforementioned delineation of responsibilities shall be added explicitly in the agreement (as an annexure) signed between the RE and the CSP. For details refer to "*Framework for adoption of cloud services for SEBI Regulated Entities*".

[9] https://www.fsb.org/wp-content/uploads/P130423-3.pdf
[10] Refer Q 3. In CERT-In Cybersecurity directions: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

9. **ISO 27001 certification[11] –**

ISO 27001 certification is a globally recognized standard for Information Security Management Systems (ISMS) published by the International Organization for Standardization (ISO). It helps organizations become risk-aware, proactively identify, and address weaknesses and promote a holistic approach to information security.

10. **IT and Cybersecurity Data**

IT and Cybersecurity Data includes the following data (but not limited to):

a. Logs and metadata related to IT systems and their operations. However, such data should not contain the following:
   i. Any *Regulatory Data*, and
   ii. Sensitive data such as internal network architecture, vulnerability details, details of admin/ privileged users of REs, password hashes, system configuration, etc.

b. Further, it should not be ordinarily possible to generate *Regulatory Data* from IT and Cybersecurity Data.

11. **Major Change/ Major Release**

CSCRF has mandated VAPT after every major release. The following changes (including but not limited to) are broadly considered as major release(s) or major change(s):

a. Implementation of a new SEBI circular.
b. Changes in core versions of software (e.g., .net, SQL, Oracle, Java, etc.)
c. Any changes in policy of login and/ or password management.
d. Significant system modifications that alter how data is exchanged with stock exchanges (e.g., file format changes, message protocol changes, etc.).
e. Introduction of new security protocols (e.g., switching from SSL to TLS 1.3).
f. Expansion into new financial markets (e.g., adding currency trading).
g. Implementation of new processes/ schema changes.

12. **Market Infrastructure Institutions (MIIs) –**

Stock Exchanges, Depositories and Clearing Corporations or any other institutions as specified by SEBI are collectively referred to as Market Infrastructure Institutions (MIIs). For applicability and inclusion of REs as MIIs, refer to section 2 ("*Thresholds for REs' categorization*") of CSCRF.

Box Item 1: REs under MIIs category for compliance with CSCRF

In the context of CSCRF, following REs are constituted as MIIs:

1. *Stock Exchanges*
2. *Depositories*
3. *Clearing Corporations*
4. *KRAs*
5. *QRTAs*

All the circulars issued by SEBI on cybersecurity for MIIs shall be uniformly applicable to all the above REs.

[11] https://www.iso.org/standard/27001

13. **Principle of Least Privilege (PoLP) –**
    Principle of Least Privilege (PoLP) is an information security concept which maintains that a user or entity shall only have access to the specific data, resources and applications needed to complete its required task.

14. **Red team exercise –**
    An exercise, reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organizational missions or business processes and to provide a comprehensive assessment of the security capabilities of an organization and its systems.

15. **Regulated Entity (RE)[12] -**
    The term 'Regulated Entity' refers to SEBI registered/ recognised intermediaries (for example stock brokers, mutual funds, KYC Registration Agencies, QRTAs, etc.) and Market Infrastructure Institutions (Stock Exchanges, Depositories and Clearing Corporations) regulated by SEBI.

16. **Regulatory Data –**
    Regulatory Data includes the following (but not limited to):
    a. Data related to core and critical activities of the RE, as well as any supporting/ ancillary data impacting core and critical activities.
    b. Data w.r.t to communication between investors and REs through applications (e.g., Chat communication, messages, emails etc.).
    c. Data that is required by the laws/ regulations/ circulars, etc. issued by SEBI and Govt. of India from time to time.
    d. Data that is deemed necessary or sensitive by the RE/ SEBI/ central or state government.
    e. The *Regulatory Data* shall be stored in an easily accessible, legible and usable form, within the legal boundaries of India. However, for the investors whose country of incorporation is outside India, the REs shall keep the data, available and easily accessible in legible and usable form, within the legal boundaries of India. Further, if the copy retained within India is not in readable format, the REs must maintain an application/system to read/ analyse the saved data.

17. **Risk –**
    As defined by OWASP[13], Risk = Likelihood × Impact; where Likelihood = Threat × Vulnerabilities. Likelihood is a measure of how likely a vulnerability is to be discovered and exploited by an attacker. Impact is the magnitude of harm that can be expected as a result from the consequences of threat exploitation.

[12] Entities within SEBI's purview, refer to Securities Contracts (Regulation) Act 1956, SEBI Act 1992, and Depositories Act 1996.
[13] Refer Risk-rating methodology: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

18. **Risk-based Authentication (RBA) –**
    Risk-based authentication is a non-static authentication mechanism that takes into account the profile of the agent requesting access to the system to determine the risk profile associated with that transaction. It checks and applies varying levels of stringency to authentication processes based on the likelihood that access to a given system could result in it being compromised.

19. **Root Cause Analysis (RCA) –**
    A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.

20. **Secure Software Development Life Cycle (SSDLC) –**
    Secure Software Development Life Cycle (SSDLC) involves integrating security testing at every stage of software development, from design, to development, to deployment and beyond.

21. **Software Bill of Materials (SBOM) –**
    A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.

22. **Trusted Channels –**
    A protected communication link established between the cryptographic module and a sender or receiver (including another cryptographic module) to securely communicate and verify the validity of plaintext CSPs, keys, authentication data, and other sensitive data. It is also called a secure channel.

1. Introduction

Technology adoption by SEBI Regulated Entities (REs) has increased manifolds in the recent years. With the fast pace of technological developments in securities market, maintaining robust cybersecurity and cyber resilience to protect the operations of REs from cyber-risks and cyber incidents has become necessary. SEBI has issued cybersecurity and cyber resilience frameworks for various REs since 2015. After taking into consideration latest trends and evolving standards, Cybersecurity and Cyber Resilience Framework (CSCRF) has been formulated to consolidate and strengthen the prevention, preparedness, and response capabilities against cyber-risks and cyber incidents.

1.1. CSCRF is based on five cyber resiliency goals namely **Anticipate, Withstand, Contain, Recover, and Evolve**.

i. **ANTICIPATE -** Maintain a state of informed preparedness in order to forestall compromises of mission/ business functions from adversary attacks.

ii. **WITHSTAND -** Continue essential mission/business functions despite successful execution of an attack by an adversary.

iii. **CONTAIN -** Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber-attacks.

iv. **RECOVER -** Restore mission/ business functions to the maximum extent possible, subsequent to successful execution of an attack by an adversary.

v. **EVOLVE -** To change mission/ business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks.

The cyber resiliency goals have been mapped to cybersecurity functions in CSCRF. The framework is broadly based on two approaches: cybersecurity and cyber resilience. Cybersecurity approach covers various aspects from governance to operational controls (including Identify, Detect, Protect, Respond, and Recover) and the cyber resilience goals include Anticipate, Withstand, Contain, Recover, and Evolve.

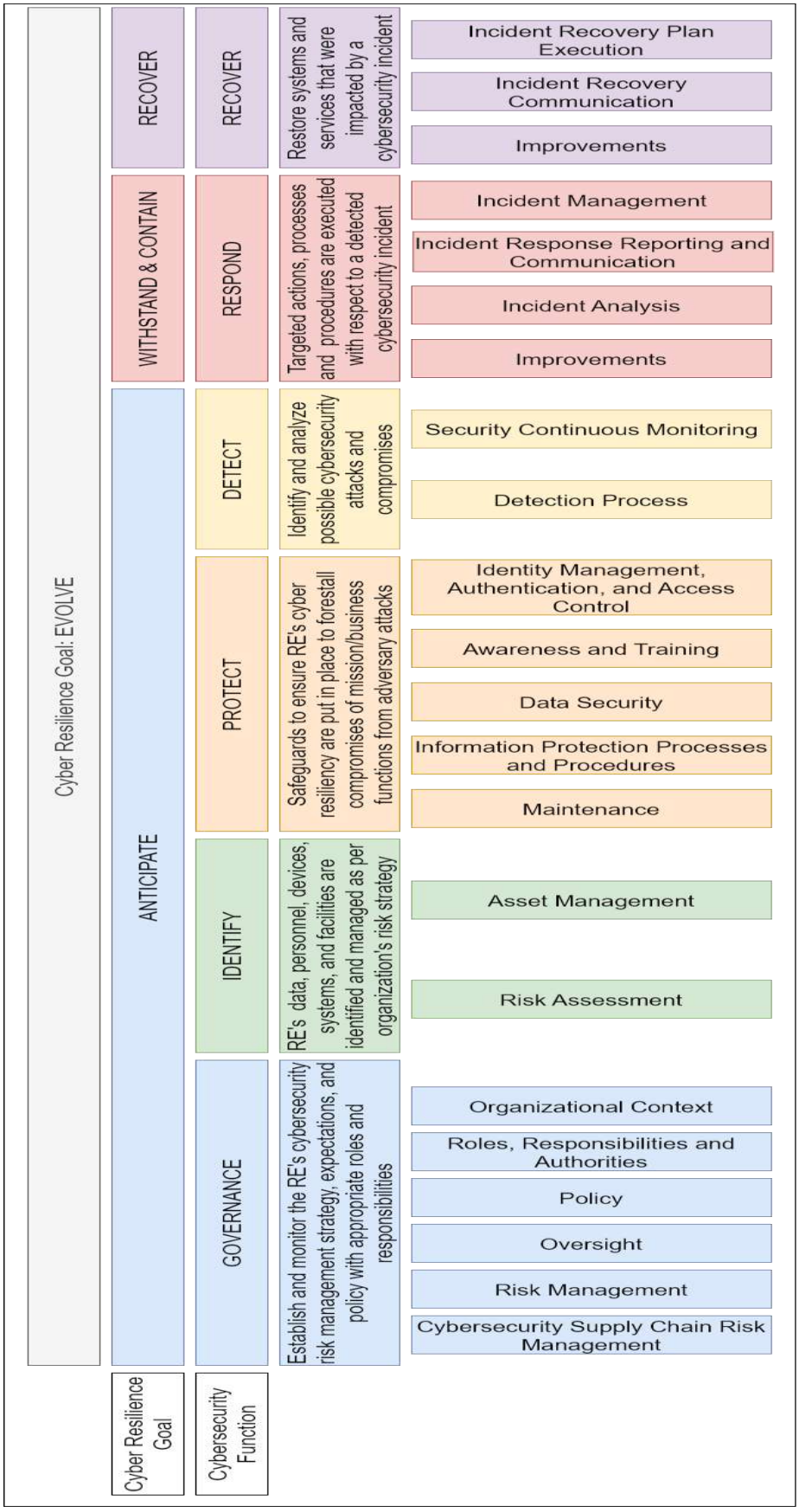

Figure 1: CSCRF Overview

The cyber resiliency goals cover different cybersecurity functions. These functions are to be implemented by REs through various cybersecurity controls. The controls are divided into the following three categories:

i. **Objectives:** The objectives highlight goals, which a security control needs to achieve.
ii. **Standards:** The standards represent established principles for compliance with CSCRF.
iii. **Guidelines:** The guidelines recommend measures for complying with standards mentioned in this document. However, few of the guidelines are mandatory in nature and shall be complied by REs as applicable.

Accordingly, the CSCRF document is divided into four parts:

i. Part I: Objectives and Standards
ii. Part II: Guidelines
iii. Part III: Compliance Formats
iv. Part IV: Annexures and References

For ease of compliance, REs are required to comply with the standards and mandatory guidelines as mentioned in the CSCRF.

Since new standards and controls have been added in CSCRF, a glide-path for adoption of CSCRF provisions has been provided as under:

i. For six categories of REs where cybersecurity and cyber resilience circular already exists – by January 01, 2025.
ii. For other REs where CSCRF is being issued for the first time – by April 01, 2025.

Accordingly, the following SEBI circulars/ guidelines/ letters/ advisories shall be deprecated as per the above-mentioned timelines.

Table 1: List of SEBI cybersecurity circulars to get supersede with CSCRF

S. No.	Regulated Entity	Circular Subject (Circular Number)	Date of issuance
1.	MIIs	Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories (*CIR/MRD/DP/13/2015*)	July 06, 2015
		Modification in Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories (*SEBI/HO/MRD1/MRD1_DTCS/P/CIR/2022/68*)	May 20, 2022

S. No.	Regulated Entity	Circular Subject (Circular Number)	Date of issuance
		Modification in Cyber Security and Cyber Resilience framework for Stock Exchanges, Clearing Corporations and Depositories (*SEBI/HO/MRD/TPD/P/CIR/2023/147*)	August 24, 2023
		Guidelines for MIIs regarding Cyber Security and Cyber Resilience (*SEBI/HO/MRD/TPD/P/CIR/2023/146*)	August 29, 2023
2.	Stock Brokers / Depository Participants	Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants (*SEBI/HO/MIRSD/CIR/PB/2018/147*)	December 03, 2018
		Clarification to Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants (*CIR/HO/MIRSD/DOS2/CIR/PB/2019/038*)	March 15, 2019
		Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants – Clarifications (*SEBI/HO/MIRSD/DOP/CIR/P/2019/109*)	October 15, 2019
		Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants (*SEBI/HO/MIRSD/TPD/P/CIR/2022/80*)	June 07, 2022
		Modification in Cyber Security and Cyber resilience framework for Stock Brokers / Depository Participants (*SEBI/HO/MIRSD/TPD/P/CIR/2022/93*)	June 30, 2022
3.	Mutual Funds / Asset Management Companies (AMCs)	Cyber Security and Cyber Resilience framework for Mutual Funds / Asset Management Companies (AMCs) (*SEBI/HO/IMD/DF2/CIR/P/2019/12*)	January 10, 2019
		Modification in Cyber Security and Cyber Resilience Framework of Mutual Funds/ Asset Management Companies (AMCs) (*SEBI/HO/IMD/IMD-I/DOF2/P/CIR/2022/81*)	June 09, 2022
4.	KYC Registration Agencies (KRAs)	Cyber Security &Cyber Resilience framework for KYC Registration Agencies (*SEBI/HO/MIRSD/DOP/CIR/P/2019/111*)	October 15, 2019

S. No.	Regulated Entity	Circular Subject (Circular Number)	Date of issuance
		Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies(KRAs) (*SEBI/HO/MIRSD/DoP/P/CIR/2022/74*)	May 30, 2022
		Modification in Cyber Security and Cyber resilience framework of KYC Registration Agencies (KRAs) (*SEBI/HO/MIRSD/TPD/P/CIR/2022/95*)	July 05, 2022
5.	Qualified Registrars to an Issue / Share Transfer Agents (QRTAs)	Cyber Security and Cyber Resilience framework for Registrars to an Issue/ Share Transfer Agents (hereinafter referred to as RTAs) (*SEBI/HO/MIRSD/CIR/P/2017/100*)	September 08, 2017
		Cyber Security & Cyber Resilience framework for Qualified Registrars to an Issue / Share Transfer Agents (*SEBI/HO/MIRSD/DOP/CIR/P/2019/110*)	October 15, 2019
		Modification in Cyber Security and Cyber resilience framework of Qualified Registrars to an Issue and Share Transfer Agents(“QRTAs”) (*SEBI/HO/MIRSD/MIRSD_RTAMB/P/CIR/2022/73*)	May 27, 2022
		Modification in Cyber Security and Cyber resilience framework of Qualified Registrars to an Issue and Share Transfer Agents (“QRTAs”) (*SEBI/HO/MIRSD/TPD/P/CIR/2022/96*)	July 06, 2022
6	Portfolio Managers	Cyber Security and Cyber Resilience framework for Portfolio Managers (*SEBI/HO/IMD/IMD-PoD-1/P/CIR/2023/046*)	March 29, 2023
7	All Regulated Entities	Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices (*SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032*)	February 22, 2023
8	Stock Exchanges, Clearing Corporations and Depositories (except Commodities	Cyber Security Operations Center for SEBI registered intermediaries (*CIR/MRD/CSC/151/2018*)	December 14, 2018

S. No.	Regulated Entity	Circular Subject (Circular Number)	Date of issuance
	Derivatives Exchanges and their Clearing Corporations)		

Table 2: List of SEBI cybersecurity letters/ advisories to get supersede with CSCRF

S. No.	Entity to which letter is issued	Letter Subject (Letter Number)	Date of issuance
1.	National Stock Exchange of India Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063905/1*)	December 26, 2022
2.	Bombay Stock Exchange of India	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063956/1*)	December 26, 2022
3.	Central Depository Services Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063931/1*)	December 26, 2022
4.	Indian Clearing Corporation Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063935/1*)	December 26, 2022
5.	Multi-Commodity Exchange of India Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063943/1*)	December 26, 2022
6.	Multi-Commodity Exchange Clearing Corporation of India Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063947/1*)	December 26, 2022
7.	Metropolitan Stock Exchange of India Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063939/1*)	December 26, 2022
8.	National Commodity Clearing Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063950/1*)	December 26, 2022

S. No.	Entity to which letter is issued	Letter Subject (Letter Number)	Date of issuance
9.	National Commodities Derivatives Exchange Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063944/1*)	December 26, 2022
10.	NSE Clearing Limited (Formerly known as National Securities Clearing Corporation Ltd.)	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063951/1*)	December 26, 2022
11.	National Securities Depositories Ltd.	Submission of Cyber Audit Report (*SEBI/HO/ITD/ITD_INSADT_D/P/OW/2022/0000063954/1*)	December 26, 2022
12.	MIIs	Recommendations of High Powered Steering Committee – Cyber Security in meeting dated February 21, 2019 (*SEBI/HO/MRD/CSC/OW/P/2019/10055/5*)	April 22, 2019
13.	Association of Mutual Funds in India (AMFI)	Review of Cyber Security and Cyber Resilience framework for Mutual Funds/Asset Management Companies (AMCs) *(SEBI/HO/IMD/IMD-TPD-1/P/OW/2023/16538)* All letters with subject '*Review of Cyber Security and Cyber Resilience framework for Mutual Funds/Asset Management Companies (AMCs)*' dated April 19, 2023 issued to Mutual Funds/AMCs or Trustee Services shall be superseded with CSCRF.	April 19, 2023
14.	Association of Mutual Funds in India (AMFI)	Review of Cyber Security and Cyber Resilience framework for Mutual Funds/Asset Management Companies (AMCs) (*SEBI/HO/IMD/IMD-SEC-3/P/OW/2023/22970/1*)	June 06, 2023

S. No.	Entity to which letter is issued	Letter Subject (Letter Number)	Date of issuance
15.	National Stock Exchange of India Ltd.	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28528/1*)	October 30, 2019
16.	Bombay Stock Exchange of India	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28516/1*)	October 30, 2019
17.	Central Depository Services Ltd.	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28517/1*)	October 30, 2019
18.	Indian Clearing Corporation Ltd.	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28523/1*)	October 30, 2019
19.	Metropolitan Stock Exchange of India Ltd.	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28525/1*)	October 30, 2019
20.	Metropolitan Clearing Corporation of India Ltd.	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28524/1*)	October 30, 2019
21.	NSE Clearing Limited	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28526/1*)	October 30, 2019
22.	National Securities Depositories Ltd.	Implementation of Cyber Capability Index (*SEBI/HO/MRD/CSC/OW/P/2019/28527/1*)	October 30, 2019

2. Thresholds for REs' categorization:

The applicability of various standards and guidelines of CSCRF is based on different categories of REs. CSCRF follows a graded approach and classifies REs in the following five broad categories:

i. Market Infrastructure Institutions (MIIs)
ii. Qualified REs
iii. Mid-size REs
iv. Small-size REs
v. Self-certification REs

The category of REs shall be decided at the beginning of the financial year based on the data of the previous financial year. Once the category of RE is decided, RE shall remain in the same category throughout the financial year irrespective of any changes in the parameters during the financial year. The category shall be validated by the respective reporting authority at the time of compliance submission. Further, the criteria given and their thresholds for different categories will continue to be updated as and when required.

Entity-wise categorization and corresponding thresholds shall be as follows:

1. Alternative Investment Fund (AIF)

Table 3: Criteria and thresholds for AIFs categorization

Sr. No.	Criteria	Self-certification REs	Small-size REs	Mid-size REs	Qualified REs
1	AUM	Less than Rs. 100 crores	Rs. 100 crores and above but less than Rs. 500 crores	Rs. 500 crores and above but less than Rs. 1000 crores	Rs. 1000 crores and above

2. Banker to an Issue and Self-Certified Syndicate Banks (SCSBs)

Banker to Issue and Self-Certified Syndicate Banks shall submit a certificate of compliance with CSCRF to SEBI on the cybersecurity guidelines issued by RBI. Wherever the bank is a listed entity, the above-mentioned certificate of compliance shall also be intimated to Stock Exchanges.

3. Client-based and Proprietary stock brokers

Table 4: Criteria and thresholds for Client-based and proprietary stock brokers' categorization

Sr. No.	Criteria	Self-certification REs	Small-size REs	Mid-size REs	Qualified REs[14]
1	Active Client-base as per UCC	Less than or equal to 10 ,000 active clients and not providing IBT or Algo trading facility	More than. 10,000 and up to 50,000	More than 50,000 and up to 5,00,000	More than 5,00,000
			Less than or equal to 10,000 active clients and providing IBT facility /Algo trading facility		

4. Collective Investment Scheme (CIS)

CIS shall be under Self-certification REs category.

5. Credit Rating Agency (CRA)

CRAs shall be under Self-certification REs category.

6. Custodians

Table 5: Criteria and thresholds for Custodians categorization

Sr. No.	Criteria	Small-size REs	Mid-size REs	Qualified REs
1	AUC	Less than Rs. 1 Lakh crores	Rs. 1 Lakh crores and above but less than Rs. 10 Lakh crores	Rs. 10 Lakh crores and above

7. Debenture Trustee (DT)

DTs which have not added any new issuer of listed debt security as client in the last three financial years shall be excluded from submission of compliance with CSCRF. Remaining DTs shall be under the Self-certification REs category.

8. Depository Participants (DPs)

Table 6: Criteria and thresholds for DPs categorization

Sr. No.	Criteria	Small-size REs	Mid-size REs	Qualified REs
1	Type of DP	N.A.	Non-institutional DP	Institutional DP

9. Designated Depository Participants (DDPs)

To get approval as a DDP, an entity, inter alia, is required to have valid SEBI registration as a Depository Participant (DP) as well as a Custodian. Therefore,

[14] As per SEBI circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2023/24 dated February 06, 2023, enhanced obligations and responsibilities have been casted upon Qualified Stock Brokers (QSBs) defined based on their size of operations, trading volumes, amount of client funds handled by them etc. Hence, such QSBs shall be categorized as Qualified REs.

categorization of highest category among DPs and Custodians shall be applicable to DDPs for submission of compliance with CSCRF.

10. Foreign Portfolio Investors (FPIs)

FPIs shall be excluded from submission of compliance with CSCRF.

11. Foreign Venture Capital Investors (FVCI)

FVCI shall be excluded from submission of compliance with CSCRF.

12. Investment Advisors (IAs)/ Research Analysts (RAs)

a. **Investment Advisors (IAs)**

Table 7: Criteria and thresholds for IAs categorization

Individual IAs	Non-individual IAs
Individual IAs shall be excluded from submission of compliance with CSCRF.	Non-individual IAs shall be categorized as Small-size REs.

b. **Research Analysts (RAs)**

Table 8: Criteria and thresholds for RAs categorization

All RAs who are not registered in other category of REs	Institutional RAs who are registered in other category of REs
All RAs who are not registered in other categories of REs shall be excluded from submission of compliance with CSCRF. However, SEBI SaaS circular titled "*Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions*" dated November 03, 2020 is applicable to RAs under which a declaration shall be submitted in respect of SaaS for managing their governance, risk compliance functions, and to improve their cybersecurity posture.	Institutional RAs who are registered with SEBI in other category of REs shall be classified as Qualified REs/ Mid-size REs/ Small size REs based on their categorization in their respective other REs/ group entity category.

13. KYC Registration Agencies (KRAs)

KRAs shall be treated at par with MIIs category for the applicability of the CSCRF.

14. Limited Purpose Clearing Corporation (LPCC)

LPCC shall be excluded from submission of compliance with CSCRF.

15. Merchant Bankers (MBs)

Table 9: Criteria and thresholds for MBs categorization

Sr. No.	Merchant Banker	Category for CSCRF
1	An entity or its parent/ subsidiary/ associate company which is a part of a conglomerate/ Systemically Important Financial Institutions	Qualified REs
2	MBs which are engaged in any activity pertaining to issue management inter alia Public Issues (IPOs, FPOs, IPOs by SME), Public Offers by REITs/InvITs, Buy-Back of Securities, Delisting of Equity Shares, Open Offer under SEBI (Substantial Acquisition of Shares and Takeovers) Regulations, 2011	Mid-size REs
3	All other MBs which are not covered in clause 1 & 2 of this table above.	Small-size REs

a. Wherever the MB is a listed entity, the compliance requirement shall also be intimated to Stock Exchanges.

16. Mutual Funds (MFs)/ Asset Management Companies (AMCs)

Table 10: Criteria and thresholds for MFs/ AMCs categorization

Sr. No.	Criteria	Small-size REs	Mid-size REs	Qualified REs
1	AUM	Less than Rs. 10,000 crores	Rs. 10,000 crores and above but less than Rs. 1 lakh crore	Rs. 1 lakh crores and above

17. Portfolio Managers

Table 11: Criteria and thresholds for Portfolio Managers categorization

Sr. No.	Criteria	Self-certification REs	Small-size REs	Mid-size REs	Qualified REs
1	AUM	Less than Rs. 1000 crores	Rs. 1000 crores and above but less than Rs. 3000 crores	Rs. 3000 crores and above	N.A.

18. Qualified Depository Participants (QDPs)

QDPs shall be excluded from CSCRF compliance.

19. Real Estate Investment Trust (REIT)/ Infrastructure Investment Trust (InvIT)

REITs/ InvITs shall be excluded from submission of compliance with CSCRF.

20. Registrar to an Issue and Share Transfer Agents (RTA)

Table 12: Criteria and thresholds for RTA categorization

Sr. No.	Criteria	Small-size REs	Mid-size REs	Qualified REs	MIIs
1	Servicing number of folios	10,000 and above but less than 1 crore	1 crore and above but less than 2 crore	N.A.	QRTAs

a. RTAs servicing less than 10,000 folios shall be excluded from submission of compliance with CSCRF.

21. Vault Managers

Vault Managers shall be excluded from submission of compliance with CSCRF.

22. Venture Capital Funds (VCFs) –

Table 13: Criteria and thresholds for VCFs categorization

Sr. No.	Criteria	Self-certification REs	Small-size REs	Mid-size REs	Qualified REs
1	Sum of corpus of all schemes of the VCF	Less than Rs. 100 crores	Rs. 100 crores and above but less than Rs. 500 crores	Rs. 500 crores and above but less than Rs. 1000 crores	Rs. 1000 crores and above

23. In case an RE is registered under more than one category of REs, then the provision of highest category under which such an RE falls shall be applicable to that RE.

3. IT Committee for REs

3.1. In order to address various technology related issues of REs, SEBI has issued circulars for composition of technical committees for MIIs, and MFs/ AMCs summarized as below:

Table 14: SEBI circular for REs and composition of their technical committees

S. no.	Regulated Entity	Name of the Committee	Circular subject (Circular number)	Date
1.	MIIs	Standing Committee on Technology (SCOT)	Committees at Market Infrastructure Institutions (MIIs) (*SEBI/HO/MRD/DOP2DSA 2/CIR/P/2019/13*)	January 10, 2019
			Statutory Committees at Market Infrastructure Institutions (MIIs) (*SEBI/HO/MRD/MRD-PoD-3/2024/088*)	June 25, 2024
2.	MFs/ AMCs	Technology Committee	Technology Committee for Mutual Funds/ Asset Management Companies (AMCs) (*SEBI/HO/IMD/DF2/CIR/ P/ 2019/058*)	April 11, 2019

3.2. With the rapid technological advancements, maintaining robust cybersecurity and cyber resilience has become a crucial and integral part of IT solution deployment. Hence, to strengthen the above mentioned committees with adequate knowledge base on cybersecurity matters, the above-mentioned committees, henceforth, shall also include one (01) external independent expert on cybersecurity matters.

3.3. Following the same approach as MIIs and MFs/ AMCs, rest of the REs which fall into the following categories-

i. Market Infrastructure Institutions (MIIs)
ii. Qualified REs
iii. Mid-size REs

Shall constitute an '*IT Committee*' which shall mandatorily include at least one (01) external independent expert on cybersecurity. For common reference in CSCRF, all the above-mentioned committees (SCOT, Technology Committee, and IT Committee) shall be termed as '*IT Committee for REs*'.

3.4. While it is not mandatory for Small-size REs and Self-certification REs to setup an *IT Committee for REs*, it is desirable to include and IT expert in

decision-making given the ever expanding role of IT in securities market. In the absence of *IT Committee for REs* for Small-size REs and Self-certification REs, the compliance to CSCRF shall be reviewed and approved by MD/ CEO/ Board member/ Partners/ Proprietor.

3.5. The brief[15] Terms of Reference (ToRs) of *IT Committee for REs* with respect to CSCRF shall be as follows:

i. The committee shall undertake periodic reviews of implementation of cybersecurity and cyber resilience policy of the RE.
ii. The committee shall also perform periodic reviews of cybersecurity incident (if any), its impact, RCA and plans to strengthen the cyber resilience in order to mitigate re-occurrence of such incidents in future.
iii. The committee shall deliberate on the matters which may be referred by the Board/ Partners/ Proprietor of the RE and/ or SEBI.
iv. The committee shall review various compliances as part of CSCRF and make recommendations to the Board/ Partners/ Proprietor of the RE.

[15] In case of existing SCOT/ IT Committees, the above-mentioned ToRs shall be considered as an addendum (and not a replacement) to the existing ToRs of the committees.

4. CSCRF Compliance, Audit Report Submission, and Timelines:

This section provides details regarding submission of compliance with the CSCRF including ISO audit, VAPT, Cyber audit, etc. and the corresponding applicable timelines.

4.1. Compliance with the Standards/ Guidelines

Unless specified otherwise, the compliance reporting for CSCRF shall be done by the REs to their respective authority(ies) as per the existing mechanism, for example, MIIs shall submit the compliance with CSCRF to SEBI, stock brokers shall submit the compliance with CSCRF to stock exchanges, depository participants to shall submit the compliance with CSCRF to depositories, etc. Further, the compliance with the applicable standards and mandatory guidelines mentioned in CSCRF shall be as follows:

Table 15: Applicability and periodicity of standards mentioned in CSCRF

Sr. No.	Standard/ Guidelines and Clause	Applicability	Periodicity
1.	Cyber resilience third-party assessment using CCI (GV.OV.S4)	MIIs	Half-yearly
	Cyber resilience self-assessment using CCI (GV.OV.S4)	Qualified REs	Annually
2.	Submission of CCI self-assessment evidence by MIIs and Qualified REs (GV.OV.S4)	MIIs and Qualified REs	Within 15 days of completion of CCI assessment (based on the applicability defined above in point 1 and 2)
3.	REs Cybersecurity and cyber resilience policy review (GV.PO.S2)	All REs	Annually
4.	REs Cybersecurity risk management policy (GV.PO.S4)	All REs	Annually
5.	*IT Committee for REs* meeting periodicity (Guidelines for GV.PO – Guideline 9)	All REs except small-size, and self-certification REs	Quarterly
6.	REs' risk assessment (threat-based) (ID.RA.S2)	MIIs	Half-yearly
		Qualified, Mid-size REs	Annually
7.	User access rights, delegated access and	MIIs and Qualified REs	Quarterly

Sr. No.	Standard/ Guidelines and Clause	Applicability	Periodicity
	unused tokens review (PR.AA.S5)	Other REs	Half-yearly
8.	Review of privileged users' activities (PR.AA.S11)	MIIs and Qualified REs	Quarterly
		Other REs	Half-yearly
9.	Cybersecurity training program (PR.AT.S1)	All REs	Annually
10.	Review of RE's systems managed by third-party service providers (GV.SC.S4)	MIIs and Qualified REs	Half-yearly
		Other REs	Annually
11.	Functional Efficacy of SOC (DE.CM.S1 – Guideline 4)	MIIs and Qualified REs	Half-yearly
		Other REs who are utilizing third-party managed SOC or Market SOC services	Annually
12.	Red Teaming exercise (DE.DP.S4)	MIIs and Qualified REs	Half-yearly
13.	Threat hunting (DE.DP.S5)	MIIs and Qualified REs	Quarterly
14.	Cybersecurity scenario-based drill exercise for testing adequacy and effectiveness of recovery plan (RC.RP.S3)	MIIs and Qualified REs	Half-yearly
		Other REs	Annually
15.	Review of periodically and update their contingency plan, continuity of operations plan (COOP) (RS.MA.S3)	MIIs and Qualified REs	Half-yearly
		Mid-size and small-size REs	Annually
16.	Evaluation of cyber resilience posture (EV.ST.S5)	Mid-size and Small-size REs	Annually

Note: During cyber audit, auditors shall also validate the adherence to the above-mentioned periodicities.

4.2. ISO Audit and Certification

4.2.1. It is mandated (as per standard PR.IP.S16) that MIIs and Qualified REs shall obtain ISO 27001 (latest version) certification. Accordingly, all MIIs and Qualified REs shall obtain ISO 27001 within 1 year of issuance of CSCRF. The evidence of certification shall be submitted along with the cyber audit report to the authority(ies) as given below:

Table 16: Reporting authority for ISO certification evidence submission

Sr. No.	Regulated Entity	Reporting authority
1.	Stock Brokers / Depository Participants who are categorized as Qualified REs	Stock Exchanges / Depositories
2.	MIIs and rest of the Qualified REs	SEBI

4.3. VAPT[16]

The VAPT scope, periodicity and compliance has been defined in standard **DE.CM.S5** and the corresponding guidelines.

4.3.1. The VAPT reporting format has been attached at **Annexure-A**. It may be noted that along with the VAPT report, SEBI REs shall also submit the declaration from MD/ CEO (as given in **Annexure-A**). The reporting authority for VAPT report is as follows:

Table 17: Reporting authority for VAPT report submission

Sr. No.	Regulated Entity	Reporting authority
1.	Stock Brokers / Depository Participants	Stock Exchanges / Depositories
2.	IAs	BASL
3.	MIIs and rest of the REs	SEBI

4.3.2. REs shall plan their VAPT activity in the beginning of the financial year. REs shall ensure that no audit cycle shall be left unaudited (if any) due to the change in category. In all such cases, the unaudited period shall be included in the current audit cycle. The periodicity of the VAPT activity for SEBI REs shall be as follows:

Table 18: VAPT periodicity of REs

Sr. No.	Regulated Entity	Periodicity
1.	REs which have been identified as '*Protected systems*' and/ or CII by NCIIPC	At least twice One VAPT activity shall be completed (including report submission, closure, and revalidation) in each half of the financial year (April to September and October to March)

[16] Unless otherwise specified, all audits mentioned in CSCRF have to be conducted by CERT-In empanelled IS auditing organization.

2.	Rest of the REs	At least once VAPT activity shall commence in the first quarter of the financial year

4.3.3. The timeline for VAPT activity for SEBI REs shall be as follows:

Table 19: VAPT report submission and observations closure timeline

Sr. No.	Activity	Timeline
1.	Report submission of VAPT	VAPT report shall be submitted after approval from respective *IT Committee for REs*, within one (1) month of completion of VAPT activity.
2.	Closure of findings identified during VAPT activity	Within 3 months of submission of VAPT report A graded approach (based on the criticality of observations) shall be followed for closure of the observations found during VAPT.
3.	Revalidation of VAPT	Revalidation of VAPT shall be completed within 5 months of completion of VAPT.

4.3.4. The closure of vulnerabilities shall be regularly tracked by *IT Committee for REs*. Additionally, any open vulnerabilities after 3 months of VAPT activity shall be approved by *IT Committee for REs* and shall be closed before start of next VAPT exercise. REs are also expected to maintain risk register which shall be reviewed by the *IT Committee for REs*.

4.3.5. The report of revalidation of VAPT exercise, and open observations must be placed before the respective *IT Committee for REs* for their confirmation and appropriate directions.

Box Item 2: Categorisation of open observations w.r.t. VAPT and cyber audit

All open observations after follow-on audit of cyber audit and/ or VAPT shall be appropriately categorised (indicative categories are mentioned below). These open observations to be placed before the IT Committee for REs and shall be closed as per their timelines approved by the Boards/ Partners/ Proprietor.

Table 20: Indicative categories of open observations after follow-on audit

S. No.	*Category*	*Example*
1.	*Absence of security control*	*MFA not implemented*

	2.	*Security control exist but exceptions to the control*	*Data-at-rest and Data-in-motion encryption is present*
	3.	*Security control in place but not consistently implemented*	*Asset inventory is being maintained but newly onboarded assets are not inventoried due to operational issues.*

4.4. Cyber Audit

Cyber audit[17] here pertains to the audit conducted for verifying the compliance with CSCRF. MIIs and Qualified REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance with CSCRF. The dashboard, once made, shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.

Cyber audit shall cover 100% of the *critical systems* and 25% non-critical systems (chosen on a sample basis).

Box Item 3: Cyber Audit and Guidelines

To verify the REs' compliance with CSCRF, cyber audit has been mandated for applicable REs.
CSCRF includes the following:

1. *Standard format for cyber audit report*
2. *Standard format for exception reporting*
3. *Periodicity, cyber audit report submission, and observations closure timeline*
4. *Action taken on open observations in report*
5. *Auditor selection norms*
6. *IT Security Auditing Guidelines for REs*

In order to achieve uniformity in reporting across REs, the audit report format has been standardized and a standard exception reporting format has also been introduced.
It has been mandated to close all open cyber audit observations with 3 months of cyber audit report submission after approval from respective IT Committee for REs. The closure of audit observation shall be regularly tracked by IT Committee for REs. In cases of open observations, the auditor shall indicate if a follow-on audit is required to review the status of non-compliances.

4.4.1. REs shall ensure that no audit cycle shall be left unaudited (if any) due to the change in category in the beginning of the financial year. In all such cases, the unaudited period shall be included in the current audit cycle. The periodicity of conducting cyber audit for SEBI REs in a financial year shall be as follows:

Table 21: Cyber audit periodicity for REs

Sr. No.	Regulated Entity	Periodicity
1.	MIIs, Qualified REs	

[17] Unless otherwise specified, all certifications / audits mentioned in CSCRF have to be conducted by CERT-In empanelled IS auditing organization.

Sr. No.	Regulated Entity	Periodicity
2.	Mid-size REs and Small-size REs who are providing IBT or Algo trading facility	At least twice in a year
3.	Rest of the REs	At least once in a year

4.4.2. The timeline of the cyber audit for SEBI REs shall be as follows:

Table 22: Cyber audit report submission and observations closure timeline

Sr. No.	Activity	Timeline
1.	Cyber audit report submission	The final cyber audit report shall be submitted after approval from respective *IT Committee for REs*, within 1 month of completion of cyber audit.
2.	Closure of findings identified during cyber audit	Within 3 months of cyber audit report submission A graded approach (based on the criticality of observation) shall be followed for closure of the observation found during cyber audit.
3.	Follow-on audit	The follow-on audit shall be completed within 5 months of completion of cyber audit.

4.4.3. Cyber audit report shall be submitted by all applicable REs. The auditor selection norms and format for CSCRF compliance submission has been attached at **Annexure-B**. Along with the cyber audit report, SEBI REs shall also submit the required declaration from MD/ CEO (as given in **Annexure-B**).

Table 23: Reporting authority for cyber audit report submission

Sr. No.	Regulated Entity	Reporting authority
1.	Stock Brokers / Depository Participants	Stock Exchanges / Depositories
2.	IAs	BASL
3.	MIIs and rest of the REs	SEBI

4.4.4. The closure of audit observations shall be regularly tracked by *IT Committee for REs*. Additionally, all open observation after 3 months of completion of cyber audit shall be approved by *IT Committee for REs* and shall be closed before start of next audit exercise.

4.4.5. The follow-on audit report and open observations must be placed before their respective *IT Committee for REs* for their confirmation and appropriate directions.

4.4.6. REs categorised as self-certification shall be required to conduct only VAPT audit through CERT-In empanelled IS auditing organisation and no other audit is required to be conducted. Self-certification (format attached at **Annexure-P)** shall be submitted for compliance with the applicable CSCRF provisions signed by RE's authorised signatory (MD/ CEO/ Board member/ Partners/ Proprietor).

4.5. Market SOC

4.5.1. The Market SOC shall be set up in accordance with the CSCRF requirements and shall ensure that participating REs are in compliance with CSCRF as applicable to them.

4.5.2. The Market SOC shall be setup:

a. Mandatorily by NSE and BSE
b. Optionally by NSDL and/ or CDSL

4.5.3. The report of functional efficacy of Market SOC shall be provided by BSE and NSE (also NSDL and CDSL, if applicable) to SEBI on a periodic basis.

4.5.4. The timeline for setting-up of Market SOC shall be January 01, 2025.

Part I: CSCRF Objectives and Standards

The main objectives of CSCRF are to proactively strengthen the security posture of the REs and prepare the operations of the REs to withstand and recover from the cyber incidents. This section breaks down the objectives and standards as per the cyber resilience goals and cybersecurity functions that REs are expected to achieve.

1. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: GOVERNANCE

1.1. GV.OC: Organizational Context (GV.OC):

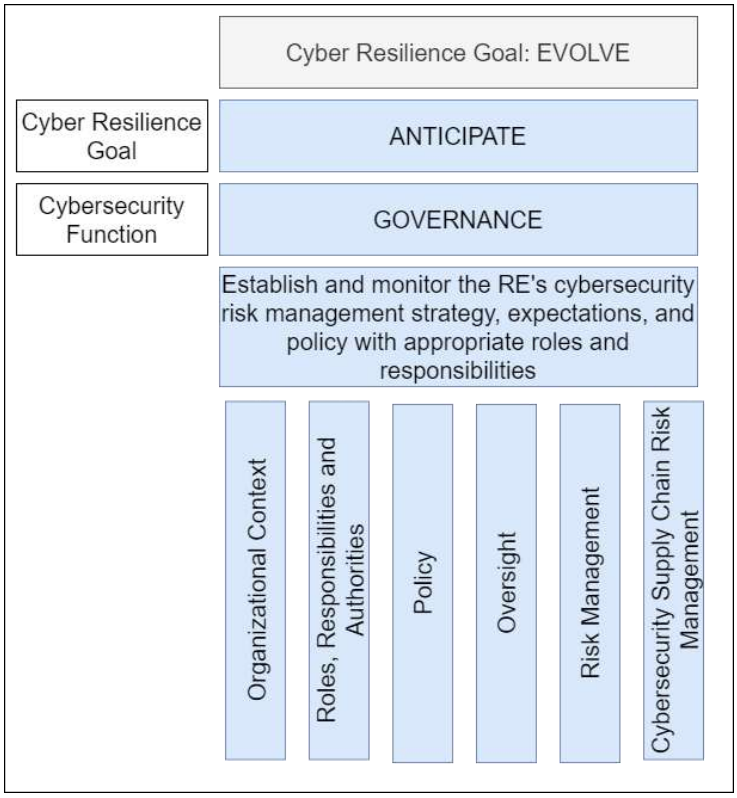

Figure 2: Overview of Governance function

i. GV.OC: Objective

The essential concomitants surrounding the REs' cybersecurity risk management decisions are understood. This includes mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements.

ii. GV.OC: Standard

1. Critical objectives, capabilities, and services that external stakeholders depend on or expect from the REs shall be understood and communicated.
2. Legal and regulatory requirements regarding cybersecurity, including data protection and data privacy, shall be understood and managed.
3. REs shall understand and communicate the outcomes, capabilities, and services dependency on external resources such as third-party service providers.

1.2. GV.RR: Roles, Responsibilities and Authorities:

i. GV.RR: Objective

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

ii. GV.RR: Standard

1. The responsibility and accountability for cybersecurity risk lies with the REs' leadership and the leadership is responsible for nurturing a culture that is risk-aware, cybersecurity conscious, and continually improving.
2. Cybersecurity risk management roles, responsibilities, and authorities shall be developed, communicated, understood, and enforced.
3. A CISO/ Designated Officer shall be appointed and report to designated authority in the organization.
4. Budgetary planning process shall be aligned with information security and privacy management objectives and processes. Adequate resources shall be allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies.
5. Employees and third-party service providers shall be allowed access to REs' information systems once they have signed a confidentiality and integrity agreement.
6. Cybersecurity shall be included in human resources training programs.

1.3. GV.PO: Policy:

i. GV.PO: Objective

Organizational cybersecurity policy is established, communicated, and enforced.

ii. GV.PO: Standard

1. A comprehensive cybersecurity and cyber resilience policy shall be documented and implemented after receiving approval from Board/ Partners/ Proprietor. The cybersecurity and cyber resilience policy shall include industry best practices, and encompass standards and guidelines mentioned in this framework.
2. The cybersecurity and cyber resilience policy shall be reviewed periodically by the REs.
3. A policy for managing cybersecurity risks shall be established based on organizational context, cybersecurity strategy, and priorities and the same shall be communicated and enforced.
4. The above-mentioned policy for managing cybersecurity risks shall be reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, and technologies.
5. Clear definition of ownership, custodian of every asset and a proper chain of command for receiving approvals shall be established and followed.

1.4. GV.OV: Oversight:

i. GV.OV: Objective

Results of organization-wide cybersecurity risk management activities, performance, and outcomes are used to inform, improve, and adjust the risk management strategy.

ii. GV.OV: Standard

1. Cybersecurity risk management strategy outcomes shall be reviewed to inform and adjust strategy and directions.
2. The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.
3. Organizational cybersecurity risk management performance is evaluated and reviewed for adjustment needed.
4. Organizations to assess their cyber resilience posture using CCI on a periodic basis.

Box Item 4: Cyber Capability Index

Under the guidance of SEBI's High Powered Steering Committing on Cybersecurity (HPSC-CS), SEBI has developed a Cyber Capability Index (CCI) for the securities market.
The above-mentioned CCI is calculated on the basis of 23 parameters with different weightages.
Based on the value of the index, the cybersecurity maturity level of the REs shall be determined as follows:

Table 24: Rating categories of REs based on CCI

SN.	***Rating***	***Index Score Rating***
1	*Exceptional Cybersecurity Maturity*	*100-91*
2	*Optimal Cybersecurity Maturity*	*90-81*
3	*Manageable Cybersecurity Maturity*	*80-71*
4	*Developing Cybersecurity Maturity*	*70-61*
5	*Bare Minimum Cybersecurity Maturity*	*60-51*
6	*Fail*	*< =50* *(RE has scored below the cut-off in at least one domain/ sub-domain)*

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

1.5. GV.RM: Risk Management:

i. GV.RM: Objective

The RE's priorities, constraints, risk tolerance and risk appetite statements, assumptions and constraints are established, communicated, and used to support operational risk decisions.

ii. GV.RM: Standard

1. REs shall prepare a cyber risk management framework to identify, assess, mitigate and monitor risks and define security processes and

procedures to address them. Cyber risk management objectives shall be agreed to by the REs' stakeholders.

2. Cybersecurity risk management activities and outcomes shall be included in risk management processes of the REs.
3. Different scenarios and their respective responses shall be documented and tested on a periodic basis to check the risk management plan of the REs.
4. Risk tolerance and risk appetite statements shall be established, communicated, and maintained. REs shall determine and clearly express their risk tolerance and risk acceptance. The risk tolerance of the REs shall be informed by their role in critical infrastructure and/ or sector specific risk analysis. REs shall maintain a risk register which shall be periodically reviewed by their *IT Committee for REs*.

Box Item 5: Cyber risk management

Cyber risk management enables an organization to identify, prioritize, manage and monitor risks to their IT/ information systems and infrastructure. Cyber risk management is a continuous and iterative process that necessitates continuous improvement and assessment of security controls by incorporating emerging new information and responding to latest threat landscape. Cyber risk management includes:

1. ***Identify:*** *Determine the threats that might affect and compromise an organization's cybersecurity. This also includes identifying cybersecurity vulnerabilities and the threats that might exploit them.*
2. ***Analyze:*** *Risk should be assessed with a measure of the likelihood of occurrence of a vulnerability and expected harmful impact that might result from the consequences of exploitation of the vulnerability.*
3. ***Evaluate:*** *Each risk should be evaluated against the threshold of acceptable risk.*
4. ***Prioritize:*** *High risk observations should be mitigated on priority.*
5. ***Respond:*** *Response to risks should be consistent with organization's Incident Response and Management Plan. Organizations may choose to treat, tolerate, terminate, transfer the risk based on their risk appetite.*
6. ***Monitor:*** *As cyber risk management is not a one-time activity but a continual process, organizations should monitor risks to ensure that they are below their pre-determined level of acceptable risk.*

1.6. GV.SC: Cybersecurity Supply Chain Risk Management:

i. GV.SC: Objective

The RE's priorities, constraints, risk tolerance, and assumptions are established and used to support decisions associated with managing supply chain risks. The RE has established and implemented the processes to identify, assess and manage supply chain risks.

ii. GV.SC: Standard

1. Cybersecurity supply chain risk management strategy/ process shall be identified, established, assessed, managed, and agreed to by organizational stakeholders.
2. Suppliers and third-party service providers of information systems, components, and services shall be identified, prioritized, and assessed using a cyber-supply chain risk assessment process.

3. Contracts with suppliers and third-party service providers shall include appropriate measures to meet the objectives of the RE's cybersecurity program and cybersecurity supply chain risk management plan (including manpower adequacy in cybersecurity domain).
4. REs shall monitor, review and ensure compliance of third-party service providers performing critical activities for their respective organization on a periodic basis.
5. SBOM shall be obtained for all new software procurements of core and critical activities and kept updated with every upgrade or change. In case the SBOM cannot be obtained for the legacy or proprietary systems, the Board/ Partners/ Proprietor of the organization shall approve the same with proper limitation, rationale, and risk management approach.
6. Response and recovery planning, and testing shall be conducted along with third-party service providers.
7. Concentration risk on outsourced agencies shall be assessed and reviewed to achieve operational resiliency.
8. Third-party service providers shall also be mandated to follow similar standards of information security.

Box Item 6: Software Bill of Materials (SBOM)

Recent security breaches at third-party vendors like Apache (Log4j), Solarwinds, etc. have led to the introduction of Software Bill of Materials (SBOM) that enables an organization to identify possible vulnerabilities in the applications/ software solutions.
With introduction of SBOM, the following benefits are envisaged for REs:

1. ***Transparency:*** *REs will become more aware of components, versions, licenses, cryptographic hashes, etc. that they are using in their software applications. This will make the REs well-informed to make better security decisions.*
2. ***Tracking vulnerabilities:*** *REs will be able to track vulnerability status for each of the components as and when an update is made or a component is added/ deleted.*
3. ***Mitigate supply chain risks:*** *REs will be able to prevent and mitigate supply chain risks arising due to open-source or third-party dependencies (e.g. libraries, repositories, etc.) in software components.*
4. ***Audit:*** *REs will have the confidence that only authorized third-party dependencies have been used in their software applications and the same can be audited as and when required.*

2. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: IDENTIFY

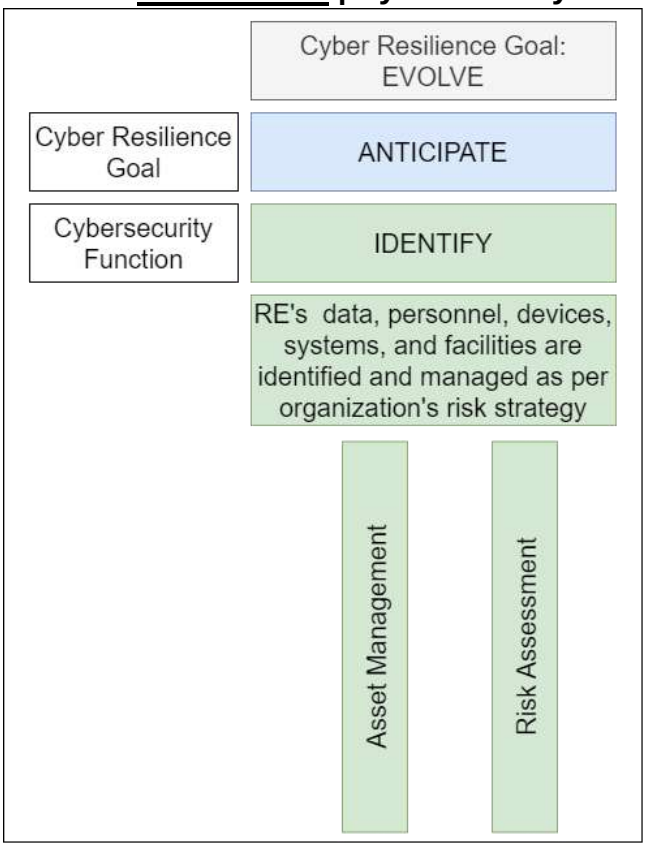

Figure 3: Overview of Identify function

2.1. ID.AM: Asset Management

i. ID.AM: Objective

The data, personnel, devices, systems, and facilities that enable the RE to achieve its business purposes are identified and managed consistently in accordance with their relative importance to organizational objectives and the RE's risk strategy.

ii. ID.AM: Standard

1. Physical devices, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets) and other interfacing systems within the organization are inventoried in a time bound manner.
2. Organizational communication, data flows and encryption methods shall be mapped and inventoried with respect to all IT systems and network resources.
3. REs shall ensure that no shadow IT assets are present in the organization.
4. Board/ Partners/ Proprietor shall approve the list of *critical systems*.
5. Inventories of data, and corresponding metadata for designated data types are maintained.

6. All inventoried IT assets and data are managed throughout their lifecycles.

2.2. ID.RA: Risk Assessment

i. ID.RA: Objective

The cybersecurity risk to the organization, assets, and individuals is assessed and understood by the RE.

ii. ID.RA: Standard

1. Asset vulnerabilities shall be identified, validated and documented. Risk factors shall be assessed and managed for all IT assets of the REs.
2. Risk assessment (including post-quantum risks[18]) of REs' IT environment shall be done on a periodic basis.
3. REs shall receive CTI from reliable/ trusted information forums and sources. REs shall be on-boarded to CERT-In Intelligence platform to receive the advisories for necessary action and implementation. Advisories issued by CERT-In/ CSIRT-Fin shall be implemented in a timely manner[19].
4. Threats, vulnerabilities, their likelihoods, and impacts shall be used to understand inherent risk and develop risk response prioritization. Vulnerabilities and cyber threats, especially related to access and authentication, along with their likelihood and potential business impacts, shall be identified and documented.
5. Risk responses shall be chosen, prioritized, planned, tracked, and communicated.

Box Item 7: Cybersecurity and Quantum Computing

Quantum Computers can efficiently break the asymmetric cryptographic systems which may jeopardize the security of transactions and expose sensitive data. Further, the symmetric cryptography may also require larger key sizes to remain secure. In view of the above, this may potentially be a major cybersecurity risk in the coming decade for the financial sector and for the REs.

To mitigate these risks, REs shall focus on the following indicative measures:

1. *REs shall maintain an inventory of cryptographic assets, prioritizing critical assets for Post Quantum Cryptography (PQC) migration, and assess their IT infrastructure capabilities.*
2. *REs shall develop strategies for the protection of assets which can and cannot be migrated to PQC.*
3. *REs shall upgrade employees' skills, periodically revise policies and conduct proof-of-concept trials in order to prepare themselves for cybersecurity challenges arising from quantum computing.*
4. *REs shall explore the feasibility to adopt PQC and technologies like Quantum Key Distribution (QKD).*

[18] Quantum computing is a rapidly emerging technology that exploits quantum mechanics' laws to solve complex problems. Post-quantum cryptography solutions can avert post-quantum risks and provide protection against quantum attacks.

[19] Within 24 hours of receiving or as indicated by SEBI.

5. *REs shall monitor ongoing quantum computing developments for cybersecurity threats, and ensure that senior management and relevant third-party service providers are aware of the possible risks associated with this technology.*
6. *REs shall enhance their crypto-agility to ensure a seamless transition to quantum-resistant solutions without disrupting their current IT systems.*

3. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: PROTECT

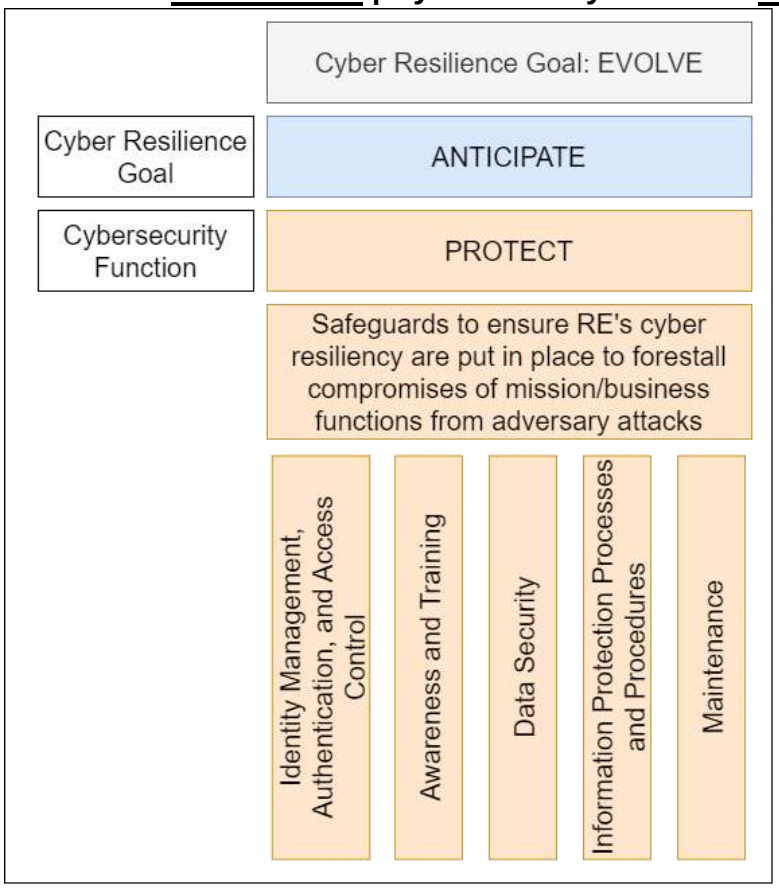

Figure 4: Overview of Protect function

3.1. PR.AA: Identity Management, Authentication, and Access Control

i. PR.AA: Objective

Access to physical and logical assets and associated facilities is limited to authorized users, processes and devices, and is managed commensurate with the assessed risk of unauthorized access.

ii. PR.AA: Standard

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
2. Network integrity is protected (through measures such as network segregation, network segmentation, etc.).
3. While granting access permissions and authorizations to resources (both on premise and cloud) of the organization, *Principle of Least Privilege* shall be followed along with segregation of duties.
4. REs shall follow Zero Trust Model to allow individuals, devices, and resources to access organization's resources.
5. Access rights shall be reviewed and documented on a periodic basis. Maker-Checker framework shall be implemented for granting, revoking, and modifying user rights in applications, databases, etc.
6. A comprehensive authentication policy shall be documented and implemented. Identities shall be proofed and bound to credentials and

asserted in interactions. Users, devices, and other assets are authenticated (single-factor or multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

7. All *critical systems* shall have MFA implemented for all users accessing from untrusted network to trusted network.
8. A comprehensive log management policy shall be documented and implemented.
9. User logs shall be uniquely identified and stored for a specified period.
10. Physical access to assets is managed, monitored, and protected. Physical access to the *critical systems* shall be monitored and recorded on a continuous basis. Individuals shall be screened before granting access to RE's organizational information and information systems.
11. Privileged users' activities shall be reviewed periodically. Access restriction shall be there for employees as well as third-party service providers. If it is required to grant access, it shall be for the limited time-period, on need-to-know basis and shall be subject to stringent supervision and monitoring.
12. Remote access to assets shall be strictly tracked and administered.
13. A comprehensive data-disposal and data-retention policy shall be documented and implemented.
14. Comprehensive SOPs shall be documented for handling storage media devices and their disposal.
15. Access control for using systems such as endpoint devices, networks, APIs, removable media, laptops, mobiles, etc. shall be defined and implemented.
16. Mobile applications shall be properly vetted against security requirements, and thoroughly tested before deployment.
17. API security with proper authentication and authorization mechanisms shall be defined and implemented.

Box Item 8: Application Programming Interface (API) security

Application Programming Interface: A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.

Application Programming Interface (API) is an interface that allows software applications to interact and communicate with each other using a set of definitions and protocols.

Since APIs have become key component of modern software application development, the practice of preventing or mitigating attacks on APIs has also become critical. API security refers to processes and solutions to mitigate vulnerabilities and risks in APIs. OWASP has released API Top 10 security threats after a sharp increase in API-related security threats.

API security guidelines broadly include the following categories:

1. ***API Discovery:*** *Knowing how many APIs are being exposed and what APIs are being used are critical steps in securing APIs.*
2. ***Access Management:*** *Enforcing strong authentication and authorization mechanisms enable secure verification of end-user client identity as well as limits the information access/ transfer to users/ systems. Implementing robust and reliable access management measures discourages use of open APIs, which*

increase the exposure and vulnerability of the data to potential breaches, fraud or misuse.

3. ***Rate Limiting:*** *Rate limiting and throttling protects bandwidth of the systems by enforcing a limit on how often an API is called and also prevents API abuse.*
4. ***Secure API development:*** *Incorporating secure-by-design strategy safeguards APIs and prevents misconfigurations and flaws.*
5. ***Zero-trust approach:*** *With zero-trust approach, API security assumes no implicit trust for any entity. Further, it also mitigates potential OWASP Top 10 API security risks.*

3.2. PR.AT: Awareness and Training

i. PR.AT: Objective

The RE's personnel and partners are provided cybersecurity awareness education, and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.

ii. PR.AT: Standard

1. Mandatory programs for building awareness of cybersecurity, cyber resilience, and system hygiene among employees shall be established. Such programs shall be conducted on a periodic basis, and shall be updated as per emergence of new threats, state-of-the-art technologies and industry trends.
2. REs shall ensure that privileged users understand their roles and responsibilities.
3. REs shall ensure that third-party stakeholders (e.g., suppliers, customers/ investors, partners) understand their roles and responsibilities.
4. REs shall ensure that senior executives/ Board members understand their roles and responsibilities. Further, a dedicated program on cybersecurity, cyber resilience, and system hygiene shall be made for Board members.
5. REs shall ensure that physical and information security personnel understand their roles and responsibilities.

3.3. PR.DS: Data Security

i. PR.DS: Objective:

Information and records (data) are managed consistent with the organization's risk strategy to protect the *Confidentiality, Integrity, and Availability* of information.

ii. PR.DS: Standard:

1. Data-at-rest and Data-in-transit shall be protected. Strong data protection measures (for both at-rest and in-transit data), with industry standard encryption algorithms, shall be put in place by all REs. Along with data-at-rest and data-in-transit, MIIs shall also explore solutions for encrypting data while it is being used/ processed.
2. REs shall classify their data into *Regulatory Data* and *IT and Cybersecurity Data* as defined in this framework. REs shall keep the *Regulatory Data* and *IT and Cybersecurity Data* available and easily

accessible in legible and usable form, within the legal boundaries of India.

3. Adequate capacity to ensure *Availability* of data shall be maintained.
4. Measures against data leaks shall be implemented. Appropriate tools shall be put in place to prevent any data leakage.
5. The development and testing environment(s) shall be separated from the production environment. For the development of critical software/ applications development, there shall be atleast one non-production environment to perform rigorous testing before deploying them to the production environment.
6. MIIs shall put in place integrity mechanisms to verify software, firmware, and information integrity of its *critical systems* and other systems connected to its *critical systems*.

Box Item 9: Data Classification

To ensure the smooth functioning of the securities market as well as sovereign control over data, SEBI has given high priority to security controls on the various kinds of data generated, managed, or processed by the REs. Taking this into consideration, CSCRF mandates REs to set up robust security controls for such data.
The data classification given below is technology agnostic, which will lead to a more enabled and strengthened environment for SEBI and REs.
CSCRF has defined the following categories of data:

1. ***Regulatory Data:*** *Regulatory Data includes the following (but not limited to):*
    a. *Data related to core and critical activities of the RE, as well as any supporting/ ancillary data impacting core and critical activities*
    b. *Data with respect to communication between investors and REs through applications (eg. chat communication, messages, emails etc.).*
    c. *Data that is required by the laws/ regulations/ circulars, etc. issued by SEBI and Govt. of India from time to time.*
    d. *Data that is deemed necessary or sensitive by the RE/ SEBI/ central or state government.*
    e. *The Regulatory Data shall be stored in an easily accessible, legible and usable form, within the legal boundaries of India. However, for the investors whose country of incorporation is outside India, the REs shall keep the original data, available and easily accessible in legible and usable form, within the legal boundaries of India. Further, if the copy retained within India is not in readable format, the REs must maintain an application/system to read/ analyse the retained data.*
2. ***IT and Cybersecurity Data:*** *IT and Cybersecurity Data includes the following data (but not limited to):*
    a. *Logs and metadata related to IT systems and their operations. However, such data should not contain the following:*
        i. *Any Regulatory Data, and*
        ii. *Sensitive data such as internal network architecture, vulnerability details, details of admin/ privileged users of REs, password hashes, system configuration, etc.*
    b. *Further, it should not be ordinarily possible to generate regulatory Data from IT and Cybersecurity Data.*

Box Item 10: Data Localization

SEBI functions to safeguard the interests of investors and promote the development of the securities market. This includes protecting the REs from all such risks which arise due to threats like single-point of failure, concentration risk, etc. While performing business activities, REs utilise services from third-party service providers. These

services include necessary software solutions hosted at the service providers' own and/ or third-party infrastructure. This could lead to business functions becoming more and more dependent on the service providers.
The hosted services/ software-as-a-service (SaaS)/ Cloud Service Providers (CSPs) usually store the data (business data, personal data etc.) where the processing of the data occurs. This results into data residing at the service providers' own and/ or third-party infrastructure.
While REs do not have a direct control on where their data is stored by the service providers, it is important to note that the REs' data may be stored on servers outside the legal boundaries of India.
If the REs' data resides outside the legal boundaries of India, SEBI and its REs may not have sovereign control on it which may cause governance issues and put limitations on the compliance of various laws related to data protection and cybersecurity in the country.
In order to protect interests of investors, and SEBI REs and their businesses, SEBI has envisaged data localization. Data localization means that all the data generated (including creation and storage) within the legal boundaries of India remains within the legal boundaries of India. Data localization ensures data sovereignty and data residency together. It will also lead to better governance and oversight.
SEBI REs shall ensure that processing and storage of data is done within legal boundaries of India. CSCRF has mandated REs to keep the original Regulatory Data available and easily accessible in legible and usable form, within the legal boundaries of India. However, for the investors whose country of incorporation is outside India, the REs shall keep the original Regulatory Data, available and easily accessible in legible and usable form, within the legal boundaries of India. Further, if the Regulatory Data retained within India is not in readable form, the REs must maintain an application/ system to read/ analyse the retained data. However, the IT and Cybersecurity Data which is to be sent to/ consumed by global/ international SOC of the REs, and SaaS based cybersecurity solutions, has been exempted from being maintained within the legal boundaries of India. For the above-mentioned SaaS based cybersecurity solutions and SOC offerings utilized by the REs (where the data is not processed/ stored within the legal boundaries of India), the IT and Cybersecurity Data sent to such solutions shall be classified, assessed and periodically reviewed (at least once in a year) by the respective IT Committee for REs or equivalent body of the RE. Additionally, such IT and Cybersecurity Data shall be approved by the Board/ Partners/ Proprietor annually.

3.4. PR.IP: Information Protection Processes and Procedures

i. PR.IP: Objective:

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

ii. PR.IP: standard:

1. A baseline configuration of IT systems shall be created and maintained incorporating security principles (e.g. concept of least functionality).
2. A System Development Life Cycle to manage systems shall be implemented.
3. REs shall put in place processes for configuration change control as well as change management.
4. REs shall thoroughly scan Critical software/ applications to ensure that no malicious code is present.

5. If the source code of software/ application is not owned by the REs, then in such a case, the REs shall obtain an undertaking/ certificate from the third-party service providers stating that their software/ application is free of known vulnerabilities, malwares, malicious/ fraudulent code and any covert channels.
6. Testing/ certification of software/ applications shall broadly address the objectives such as product/ version/ module(s) functions only in a manner that it is intended to do, it is developed as per the best secure design/ coding practices and standards, it addresses known flaws/ threats due to insecure coding, etc.
7. REs shall document backup and recovery plan of data to ensure that there is no data loss.
8. REs shall implement, test, and maintain data backups. Further, drills for restoration of backup data shall be conducted on a periodic basis.
9. Policies and regulations regarding the physical operating environment for REs' assets shall be defined and adhered to.
10. Effectiveness of protective technologies shall be measured on a regular basis in line with the SLAs.
11. Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) shall be put in place and regularly tested and updated.
12. A vulnerability management plan shall be developed and implemented.
13. For applicable cloud instances of REs, SEBI circular '*Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)*' shall be complied with.
14. Only CERT-In empanelled IS auditing organizations shall be onboarded for external audit (including cyber audit) of REs to audit the implementation of standards and mandatory guidelines (as applicable) mentioned in this framework.
15. All software services in the form of SaaS/ Hosted services, COTS, customized COTS, in-house developed software, etc. shall be certified for application security and functional audit. COTS products empanelled by stock exchanges/ depositories shall be certified for application security testing, and functional audit by STQC at the time of empanelment.
16. MIIs and Qualified REs shall obtain ISO 27001 certification.
17. MIIs and Qualified REs shall follow globally recognized standards such as CIS Critical Security Controls to enhance their cyber resilience.

3.5. PR.MA: Maintenance

i. PR.MA: Objective:

Maintenance and repairs of organizational control and information system components are performed consistent with policies and procedures.

ii. PR.MA: Standard:

1. Maintenance and repair of REs' assets shall be performed and logged, with approved and controlled tools.
2. Remote maintenance of REs' assets shall be approved, logged, and performed in a manner that prevents unauthorized access.
3. Patches shall be identified and categorized based on their severity. Critical patches shall be implemented at the earliest. Patches shall be tested in non-production environment before applying to DC and DR.

4. Cyber Resilience Goal: ANTICIPATE | Cybersecurity function: DETECT

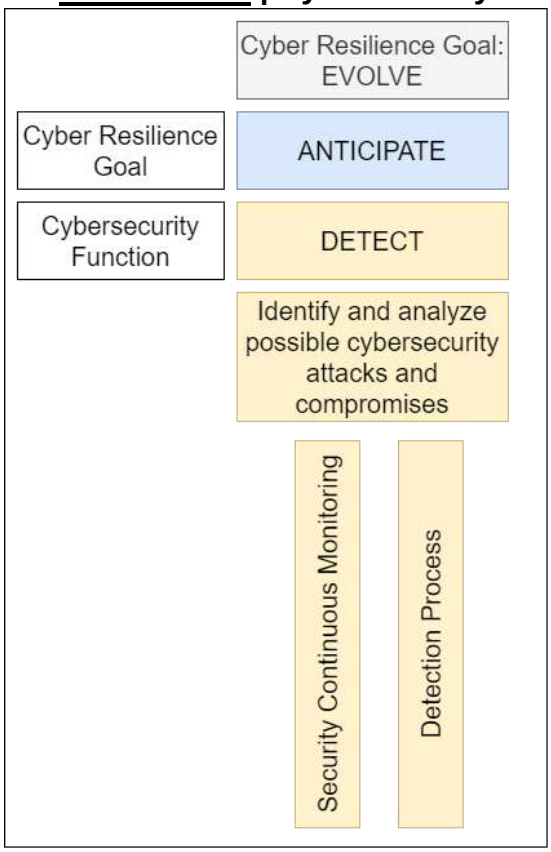

Figure 5: Overview of Detect function

4.1. DE.CM: Security Continuous Monitoring

i. DE.CM: Objective:

The REs' information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

ii. DE.CM: Standard:

1. The SOC shall cover (including but not limited to) network, endpoints, physical environment, personnel activities, malicious code, unauthorized mobile code, activities of third-party service providers, monitoring of unauthorized personnel, devices, connections and software, etc. Security Operations Centre (SOC)[20] shall be up and running 24×7×365 to monitor, prevent, predict, detect, investigate, and respond to cyber threats.
2. Appropriate continuous security monitoring mechanisms shall be established in SOC for the timely detection of anomalous or malicious activities.

[20] *SEBI through its circular CIR/MRD/CSC/148/2018 dated December 07, 2018 has mandated all stock exchanges, Clearing Corporations, and Depositories (except Commodities Derivatives Exchanges and their Clearing Corporation) to have a Cyber Security Operations Centre (C-SOC) that would be 24×7×365 set-up manned by dedicated security analysts to identify, respond, recover, and protect from cybersecurity incidents.*

3. All anomalies and alerts generated shall be properly monitored and investigated within stipulated time.
4. Capacity utilization shall be monitored for all the *critical systems* in the organization.
5. Cybersecurity audit, configuration audit, implementation audit, change management audit, and VAPT shall be conducted to detect vulnerabilities in IT environment.

Box Item 11: Security Operations Centre (SOC) and Market SOC

The key functions performed by SOC are as follows:

1. ***Continuous monitoring:*** *To monitor the end-points and network round the clock to immediately notify of abnormal or suspicious behavior.*

2. ***Log management:*** *To collect, maintain, and review logs of all end-points and network activities. Further, SOC aggregates and correlates data from various applications, firewalls, OS and endpoints to establish a baseline for normal behavior.*

3. ***Threat response:*** *To act as a first responder during a cybersecurity incident. Captive SOC is responsible to perform actions like isolating endpoints and limiting the damage with as little disruption of the business as possible. For all forms of managed SOC, the service provider shall alert the RE and guide them in incident management.*

4. ***Alert Management:*** *To monitor alerts issued by diverse tools and closely inspect each one of them in order to discard false positives (if any), and determine the potential impact of threats.*

5. ***Root Cause Investigation:*** *Post the occurrence of incident, SOC is responsible for investigating when, how and why an incident occurred. SOC analyzes all logs to identify the root cause of the incident and prevent its reoccurrence after incorporating learnings from the incident.*

While SOC serves twofold purpose, i.e., assessing and alerting security threats in real time thereby continuously improving organization's security posture, however, setting-up own SOC may be onerous for the small REs. Therefore, to improve the cybersecurity posture of such REs, CSCRF provides setting different types of SOC. CSCRF has mandated SOC for all REs (except client-based stock brokers having less than 100 clients). However, CSCRF allows REs to choose any one of the below models to utilize SOC services:

1. *RE's own/ group SOC*
2. *Market SOC implemented mandatorily by NSE, BSE and optionally by NSDL and/ or CDSL*
3. *Any other third-party managed SOC*

Small-Size and Self-certification category REs are mandated to be on-boarded on above-mentioned Market SOC.

SEBI's expectations from Market SOC are as follows:

1. *To provide cyber hygiene for Indian securities market ecosystem by providing cost-effective solutions.*
2. *For small-size and mid-size REs, Market SOC shall also provide services of VAPT and cyber audit at an affordable cost. Further, the above-mentioned VAPT and cyber audit should be conducted by a CERT-In empanelled IS Auditing Organization.*

The particulars of the Market SOC shall be as follows:

1. *The Market SOC shall be setup:*
   a. *Mandatorily by NSE and BSE*

b. Optionally by NSDL and/ or CDSL

2. *The Market SOC shall be set up in accordance with the CSCRF requirements and shall ensure that participating REs are in compliance with CSCRF as applicable to them.*
3. *The Market SOC shall bridge technological gap for small REs and provide them robust SOC services. However, the responsibility and accountability for compliance with CSCRF rests with the REs.*
4. *The Market SOC shall evolve continuously in order to incorporate new security controls and guidelines that may be issued by SEBI from time to time.*
5. *The Market SOC provider shall ensure that the REs participating in their SOC adhere to the minimum IT guidelines and security protocols all the time.*
6. *NSE and BSE (NSDL and CDSL, if applicable) shall carry out audit of their Market SOC activity annually and submit the report to SEBI.*

*Functional efficacy of market SOC shall be measured in accordance with **Annexure-N** of CSCRF and shall be reported along with market SOC providers' cyber audit report.*

4.2. DE.DP: Detection Process

i. DE.DP: Objective

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

ii. DE.DP: Standard

1. Roles and responsibilities for detection are defined to ensure accountability.
2. REs shall ensure that detection processes are tested by developing playbooks and use-cases.
3. Event detection information shall be communicated as per the regulatory requirements and organizational policies.
4. MIIs and Qualified REs shall conduct goal-based adversarial simulation red teaming exercise on a periodic basis to identify potential weaknesses within the organization's cyber defense.
5. REs shall conduct threat hunting and compromise assessment on a regular basis.

5. Cyber Resilience Goal: WITHSTAND & CONTAIN | Cybersecurity function: RESPOND

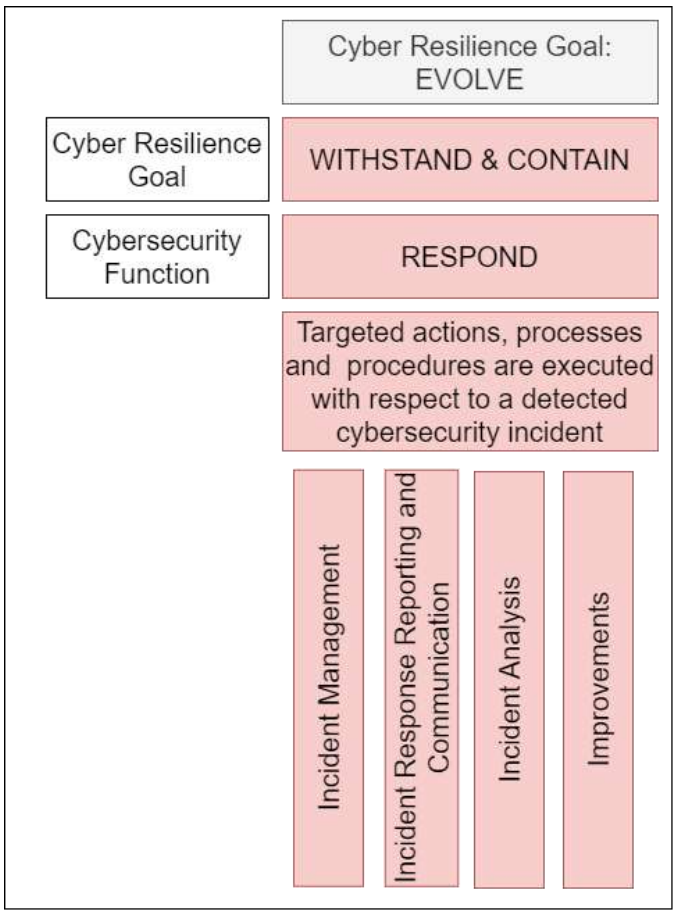

Figure 6: Overview of Respond function

5.1. RS.MA: Incident Management

i. RS.MA: Objective:

Incident response plans and procedures are executed and maintained in order to ensure response to detected/ known cybersecurity incidents.

ii. RS.MA: Standard:

1. A comprehensive CCMP shall be documented with scenario-based SOP. Further, incident response management plan shall also be a part of CCMP. Additionally, response plan and execution of required SOP shall be triggered as soon as an incident occurs.
2. REs shall optimize their ability to respond in a timely and appropriate manner to adverse conditions, stresses, attacks, or indicators of these. This will maximize the REs' ability to maintain business operations, limit consequences, and avoid destabilization.
3. REs shall prepare contingency plans, COOP, training, exercises, and incident response and recovery plans for their systems and infrastructure and get them approved from their respective Board/ Partners/ Proprietor.

4. Cybersecurity incidents shall be contained and mitigated. Further, newly identified vulnerabilities shall be mitigated or documented as accepted risks.
5. MIIs and Qualified REs shall get onboarded to CSK (Cyber Swachhta Kendra) and other CERT-In initiatives as notified from time to time.

Box Item 12: Cybersecurity Incidents – Classification and Response

- *CSCRF has classified cybersecurity incidents into four categories:*
  1. *Low severity*
  2. *Medium severity*
  3. *High severity*
  4. *Critical severity*
- *Cybersecurity incident response process can be divided into several phases. Cyber incident response handling can be divided into four broad phases:*
  1. ***Preparation:*** *This phase covers not only establishment of incident response capabilities to ensure RE's readiness to respond to incidents but also prevention of incidents by having secure systems, networks, and applications. CSCRF has mandated REs to have an effective policy, response plan/strategy, communication, and documentation.*
  2. ***Detection and Analysis:*** *Detection and analysis phase involves:*
     i. *Collection of data and logs*
     ii. *Identification of IOAs*
     iii. *Identifying a baseline for normal behavior, and*
     iv. *Correlating events to check deviation in behavior.*
  3. ***Containment, Eradication & Recovery:*** *The objective of containment is to mitigate the incident before it overwhelms RE's resources and causes more damage. In eradication and recovery phase, all affected systems shall be isolated from the RE's network. Once the affected systems have been isolated, remediation steps should be taken to resume normal operations.*
  4. ***Post-incident activity:*** *Lessons learned should be shared within the organization to improve the RE's security measures and incident handling process.*
- *CSCRF covers aforementioned incident handling process through various standards and guidelines, and ensures that REs become more cyber resilient and provide a better response to cybersecurity incidents. Further, timelines for handling cyber incidents and report submission have also been provided in this framework.*

5.2. RS.CO: Incident Response Reporting and Communication

i. RS.CO: Objective:

Response activities are coordinated with internal and external stakeholders (e.g. external support from CERT-In, law enforcement agencies, etc.). Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

ii. RS.CO: Standard:

1. An SOP, documenting the roles and responsibilities of REs' personnel (with respect to cybersecurity incident response*),* shall be prepared and implemented.
2. Any cybersecurity incident falling under CERT-In Cybersecurity directions[21] shall be notified to SEBI, CERT-In, and NCIIPC (as

[21] Refer Q 30 in CERT-In Cybersecurity directions: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

applicable) within a stipulated time. Any/ all other cybersecurity incident(s) shall be reported to SEBI, CERT-In and NCIIPC (as applicable) as per guidelines.

3. In the event of a cybersecurity incident, REs shall coordinate with stakeholders as per their CCMP.

5.3. RS.AN: Incident Analysis

i. RS.AN: Objective:

Incident analysis is conducted to ensure effective response and support recovery activities.

ii. RS.AN: Standard:

1. Processes shall be established to receive, analyze and respond to vulnerabilities/ incidents disclosed to the RE from internal and external sources (e.g. internal testing, security bulletins, or security researchers).
2. Cybersecurity incidents shall be categorized in-line with categorization given in RE's CCMP.
3. Detailed investigation of cybersecurity incidents, and alerts as well as a forensic analysis (as appropriate) shall be done to identify the root-cause of the incident, the modus operandi of the threat actor, lateral movement of the threat actor (if any), and to prevent the reoccurrence of similar incidents.
4. RCA shall be done to:
   a. Determine the gaps in terms of people, processes, and technology that led to the incident, and
   b. Further enhance the RE's security posture to prevent/ mitigate similar cybersecurity Incidents in the future.
5. Impact analysis of the incident shall be mandatorily conducted by the REs. Further, RCA and forensics analysis (as appropriate) shall be performed as per '*Classification and Handling of Cybersecurity Incidents*' SOP attached at **Annexure-O**.

5.4. RS.IM: Improvements

i. RS.IM: Objective:

RE's response activities are improved by incorporating lessons learned from current and previous detection/ response activities.

ii. RS.IM: Standard:

1. Lessons learned from incident handling activities shall be incorporated into incident response plans, training, and testing, and resulting changes shall be implemented accordingly.
2. Changes to the response plan shall be communicated to RE's designated key personnel.

6. Cyber Resilience Goal: RECOVER | Cybersecurity function: RECOVER

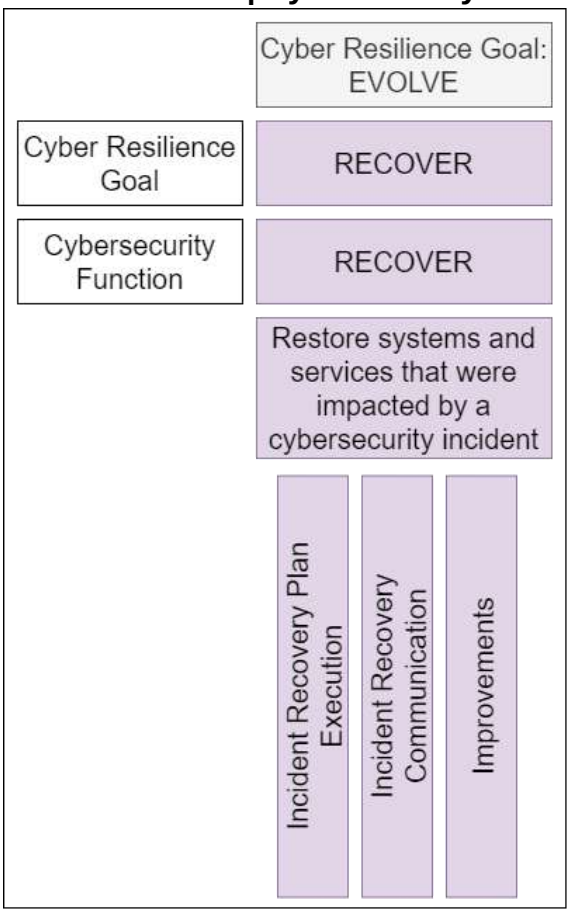

Figure 7: Overview of Recover function

6.1. RC.RP: Incident Recovery Plan Execution

i. RC.RP: Objective:

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity incidents.

ii. RC.RP: Standard:

1. Recovery plan of REs shall have different cyber-scenario based classifications.
2. RTO and RPO, as specified by SEBI, shall be mandated while executing recovery plan for the restoration of systems after a cybersecurity incident.
3. REs shall periodically conduct drills for testing different recovery scenarios.
4. Backup and recovery plan of data shall be documented to ensure that there is no data loss.

6.2. RC.CO: Incident Recovery Communication

i. RC.CO: Objective:

Restoration activities are coordinated with internal and external stakeholders.

ii. RC.CO: Standard:

1. Public relations management as defined in the recovery plan shall be undertaken in the event of a cybersecurity incident.
2. REs shall communicate recovery activities to internal and external stakeholders as well as executive and management teams.
3. REs shall inform actions taken during recovery process to all related stakeholders.

6.3. RC.IM: Improvements

i. RC.IM: Objective:

Recovery planning and processes are improved by incorporating lessons learned from execution of recovery plans and processes.

ii. RC.IM: Standard:

1. Recovery plans shall be updated and improved to incorporate lessons learned from cybersecurity incidents.
2. REs cyber resilience capabilities shall be upgraded through periodic drills to ensure safe and timely restoration of critical operations.

7. Cyber Resilience Goal: EVOLVE

Figure 8: Overview of Evolve goal

7.1. EV.ST: Strategies

i. EV.ST: Objective

A major component of cyber resilience is the ability to adapt and improve the security posture to stay ahead of threats.

ii. EV.ST: Standard

1. REs shall formulate strategies to anticipate new attack vectors by removing or applying new controls to compensate for identified vulnerabilities or weaknesses, reducing or manipulating attack surfaces, and proactively orienting controls, practices, and capabilities to prospective, emerging, or potential threats.
2. REs shall demonstrate heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.
3. REs shall confirm post-incident modification of business functions and supporting processes to handle adversity and address environmental changes more effectively. In case of a cybersecurity incident, learning shall be incorporated to improve and evolve their cyber resilience posture.
4. MIIs and Qualified REs shall continuously adapt and evolve to counter new cybersecurity threats and challenges.
5. Mid-size and Small-size REs shall periodically evaluate their cyber resilience posture.

8. Exemption Table

8.1. Self-certification REs and small-size REs shall be exempted from compliance with standards mentioned below in Table 25. Following exemptions shall be applicable for small-size REs and self-certification REs provided they are onboarded to Market SOC.

Table 25: Standards exempted for Self-certification REs and small-size REs

S.no	Standard Code	Standard name
1.	GV.OC.S1	Governance: Organizational Context – Standard 1
2.	GV.OC.S3	Governance: Organizational Context – Standard 3
3.	GV.RR.S1	Governance: Roles, Responsibilities and Authorities – Standard 1
4.	GV.RR.S4	Governance: Roles, Responsibilities and Authorities – Standard 4
5.	GV.RR.S5	Governance: Roles, Responsibilities and Authorities – Standard 5
6.	GV.OV.S1	Governance: Oversight – Standard 1
7.	GV.OV.S2	Governance: Oversight – Standard 2
8.	GV.OV.S3	Governance: Oversight – Standard 3
9.	GV.OV.S4	Governance: Oversight – Standard 4
10.	GV.RM.S1	Governance: Risk Management– Standard 1
11.	GV.RM.S2	Governance: Risk Management– Standard 2
12.	GV.RM.S3	Governance: Risk Management– Standard 3
13.	GV.RM.S4	Governance: Risk Management– Standard 4
14.	GV.SC.S1	Governance: Cybersecurity Supply Chain Risk Management – Standard 1
15.	GV.SC.S2	Governance: Cybersecurity Supply Chain Risk Management – Standard 2
16.	GV.SC.S3	Governance: Cybersecurity Supply Chain Risk Management – Standard 3
17.	GV.SC.S6	Governance: Cybersecurity Supply Chain Risk Management – Standard 6
18.	GV.SC.S7	Governance: Cybersecurity Supply Chain Risk Management – Standard 7
19.	ID.AM.S2	Identify: Asset Management – Standard 2
20.	ID.AM.S6	Identify: Asset Management – Standard 6
21.	ID.RA.S1	Identify: Risk Assessment– Standard 1
22.	ID.RA.S2	Identify: Risk Assessment– Standard 2
23.	ID.RA.S3	Identify: Risk Assessment– Standard 3
24.	ID.RA.S5	Identify: Risk Assessment – Standard 5
25.	PR.AA.S4	Protect: Identity Management, Authentication, Access Control – Standard4
26.	PR.AA.S15	Protect: Identity Management, Authentication, Access Control – Standard15
27.	PR.AA.S16	Protect: Identity Management, Authentication, Access Control – Standard16
28.	PR.AA.S17	Protect: Identity Management, Authentication, Access Control – Standard17

S.no	Standard Code	Standard name
29.	PR.DS.S1	Protect: Data Security – Standard 1
30.	PR.DS.S5	Protect: Data Security – Standard 5
31.	PR.DS.S6	Protect: Data Security – Standard 6
32.	PR.IP.S3	Protect: Information Protection Processes and Procedures – Standard 3
33.	PR.IP.S16	Protect: Information Protection Processes and Procedures – Standard 16
34.	PR.IP.S17	Protect: Information Protection Processes and Procedures – Standard 17
35.	PR.MA.S1	Protect: Maintenance – Standard 1
36.	PR.MA.S2	Protect: Maintenance – Standard 2
37.	DE.CM.S4	Detect: Security Continuous Monitoring – Standard 4
38.	DE.DP.S4	Detect: Detection Process – Standard 4
39.	DE.DP.S5	Detect: Detection Process – Standard 5
40.	RS.MA.S2	Respond: Incident Management – Standard 2
41.	RS.MA.S3	Respond: Incident Management – Standard 3
42.	RS.MA.S5	Respond: Incident Management – Standard 5
43.	EV.ST: S1	Evolve: Strategies – Standard 1
44.	EV.ST: S2	Evolve: Strategies – Standard 2
45.	EV.ST: S3	Evolve: Strategies – Standard 3
46.	EV.ST: S4	Evolve: Strategies – Standard 4

Along with Standards mentioned in Table 25, Self-certification REs shall be exempted from compliance to periodic cyber audit by CERT-In empanelled IS auditing organizations, i.e., Protect – Information Protection Processes and Procedures – Standard 14 (PR.IP.S14) and periodic evaluation of cybersecurity posture – Evolve – Strategies -Standard 5 (EV.ST.S5).

8.2. Mid-size REs shall be exempted from compliance to standards mentioned below in Table 26. Following exemptions shall be applicable mid-size REs provided they are onboarded to Market SOC.

Table 26: Standards exempted for Mid-size REs

S.no	Standard Code	Standard name
1.	GV.OV.S4	Governance: Oversight – Standard 4
2.	ID.RA.S3	Identify: Risk Assessment – Standard 3
3.	PR.DS.S5	Protect: Data Security – Standard 5
4.	PR.DS.S6	Protect: Data Security – Standard 6
5.	PR.IP.S16	Protect: Information Protection Processes and Procedures – Standard 16
6.	PR.IP.S17	Protect: Information Protection Processes and Procedures – Standard 17
7.	DE.DP.S4	Detect: Detection Process – Standard 4
8.	DE.DP.S5	Detect: Detection Process – Standard 5
9.	RS.MA.S5	Respond: Incident Management – Standard 5

Part II: CSCRF Guidelines

This section contains CSCRF guidelines that provides a direction to REs for the implementation of standards mentioned in CSCRF. There are certain guidelines which are mandatory in nature and have been written under '*Applicability*' column (Refer section 2 "*Thresholds for REs' categorization*").

Standards	CSCRF guidelines	Applicability
Cyber Resilience goal: ANTICIPATE		
Cybersecurity control: GOVERNANCE		
GV.OC: Guidelines		
GV.OC.S2, GV.OC.S3	1. Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. 2. To ensure the goal of cybersecurity, REs shall define responsibilities of its own employees, third-party service providers' employees, and other entities, who may have privileged access or use their systems/ networks.	All REs except small-size, self-certification REs
GV.OC.S2	1. All REs shall understand, manage and comply with relevant cybersecurity and data security/ protection requirements mentioned in government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/ circular/ regulation as and when issued. 2. Conduct audits and inspections of IT resources of REs (and its sub-contractors/ third-party service providers) or engage third-party auditor to conduct the same and check the adherence with SEBI and government guidelines/ policies/ laws/ circulars/ regulations, etc., and standard industry practices. 3. SEBI/ any other government agency shall at any time perform search and seizure of RE's IT resources storing/ processing data and other relevant IT resources (including	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	but not limited to logs, user details, etc.) pertaining to the RE. In this process, SEBI or SEBI authorized personnel/ agency may access RE's IT infrastructure, applications, data, documents, including other necessary information given to, stored or processed by third-party service providers. 4. Engage a forensic auditor to identify the root cause of any incident (cybersecurity or other incidents) related to RE. 5. SEBI shall seek the audit reports of the audits conducted by RE.	
GV.RR: Guidelines		
GV.RR.S3	1. REs shall designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/ Partners/ Proprietor of the MII and qualified REs. The reporting of the CISO of the MII and Qualified REs shall be directly to the MD & CEO of their organization. CISO shall possess sufficient qualification and capabilities to carry out his/ her responsibilities. REs shall establish a reporting procedure to facilitate communication of cybersecurity incidents/ unusual activities to the CISO or to the senior management in a time-bound manner as defined by guidelines/ policies/ laws/ circulars/ regulations, etc. MIIs and REs which have been identified as CII by NCIIPC shall define roles and responsibilities of CISO as per NCIIPC guidelines[22]. The level, grade, and standing of CISO shall be atleast equivalent to CTO/ CIO.	MIIs, Qualified REs (Mandatory)

[22] https://www.nciipc.gov.in/documents/Roles_Responsibilities-CISO.pdf

Standards	CSCRF guidelines	Applicability
	1. REs shall designate a senior official or management personnel (henceforth, referred to as the "Designated Officer") whose function would be to assess, identify, and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cybersecurity and cyber resilience policy approved by the Board/ Partners/ Proprietor. REs shall establish a reporting procedure to facilitate communication of cybersecurity incidents/ unusual activities to Designated Officer in a time-bound manner as defined by guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI or GoI.	Mid-size, small-size, self-certification REs (Mandatory)
GV.RR.S4	1. REs shall allocate adequate percentage of total IT budget to cybersecurity. Such allocation shall be mentioned under separate budgetary head for monitoring by the Board of directors/ top-level management. 2. REs shall ensure that adequate resources are allocated and aligned with cybersecurity risk strategy, roles and responsibilities, and policies. Resources should be defined in terms of budgetary allocation, people, and material. Resourcing requirements should be revisited regularly based upon progress or shortfalls in the implementation of standards and shall reflect in the budgetary allocation.	All REs except small-size, self-certification REs
GV.RR.S5, GV.RR.S6	1. REs shall ensure that every employee hired, irrespective of the department or role, present a low/ no threat to the REs' cybersecurity posture. This includes (but not limited to): a. Conducting due diligence b. Ensuring employees receive proper security training during onboarding and on regular basis	All REs except small-size, self-certification REs

Standards	CSCRF guidelines	Applicability
	c. Employment screening procedures, employment policies and agreement, employment termination procedures etc. are followed. 2. REs shall sign a confidentiality and integrity agreement with third-party service providers and conduct due diligence of all third-party service providers accessing their IT systems.	
GV.PO: Guidelines		
GV.PO.S1, GV.PO.S2, GV.PO.S5	1. As part of the operational risk management framework to manage risks to systems, networks and databases from cyber-attacks and threats, REs shall formulate a comprehensive Cybersecurity and Cyber Resilience policy document encompassing CSCRF. In case of deviations from the CSCRF, reasons for such deviations, technical or otherwise, shall be provided in the policy document. 2. The policy document shall be approved by the Board/ Partners/ Proprietor of the REs. The policy document shall be reviewed by the aforementioned group periodically with a view to strengthen and improve cyber resilience posture.	All REs (Mandatory)
	3. REs shall have policies (including but not limited to) with respect to asset management, patch management, vulnerability management, VAPT policy, audit policy, monitoring of the networks and endpoints, configuration management, change management, secure software development life cycle management, authentication policies, authorization policies and processes, network segmentation/ isolation policies, commissioning internet facing assets, encryption policies, PII and privacy policies, cybersecurity control management policy, asset ownership documentation, etc., and chain of command for any approval process in the organization with respect to cybersecurity. The policies shall also contain do's and don'ts in the organization with respect to usage of information assets including desktops, laptops, BYOD, networks, internet, data, etc. The	

Standards	CSCRF guidelines	Applicability
	aforementioned policies may form a part of RE's cybersecurity policy or may be standalone policies. 4. REs shall formulate a policy for mobile and web applications and associated services with the approval of their Board/ Partners/ Proprietor. The contours of the policy, while discussing the parameters of any "new product" including its alignment with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., shall explicitly include security requirements from Functionality, Security and Performance (FSP) angles. 5. All information/ data (classified as *Regulatory Data* and *IT and Cybersecurity Data*) that is consumed/ handled by REs shall be made accessible to SEBI when required. If there is any dependency on external party, REs shall facilitate information sharing with SEBI by including it in their agreement with external party.	
	6. The Cybersecurity Policy shall include the following process to identify, assess, and manage cybersecurity risks associated with processes, information, networks and systems: a. 'Identify' critical IT assets and risks associated with such assets. b. 'Protect' assets by deploying suitable controls, tools and measures. c. 'Detect' incidents, anomalies and attacks through appropriate monitoring tools/processes. d. Respond' by taking immediate steps after identification of the incident, anomaly or attack. e. 'Recover' from incident through incident management and other appropriate recovery mechanism	All REs

Standards	CSCRF guidelines	Applicability
	7. REs shall follow Plan-Do-Check-Act concept while creating and using the documented information. For example, activities under the 'Plan' phase shall be guided by Policies, the 'Do' phase will follow Procedures (SOPs), and the 'Check' and 'Act' phases will refer to the Policies and Procedures.	All REs except small-size, Self-certification REs
	8. As part of compliance management with respect to CSCRF, REs shall apply following key aspects (including but not limited to) for implementing compliance management: a. Assess Compliance with applicable guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI or GoI. b. Develop compliance policies and procedures c. Implement controls such as security measures d. Train employees e. Monitor and review compliance management processes f. Regular audits and reporting.	All REs except small-size, Self-certification REs
	9. The Board/ Partners/ Proprietor of the REs shall constitute an *IT Committee for REs* comprising experts proficient in technology. This IT Committee of REs shall meet on a periodic[23] basis to review the implementation of the cybersecurity and cyber resilience policy approved by their Board/ Partners/ Proprietor, and such review shall include goal setting for a target level of cyber resilience, and establishing a plan to improve and strengthen cybersecurity and cyber resilience. The review shall be placed before the Board/ Partners/ Proprietor of REs for appropriate action.	All REs except small-size, Self-certification REs (Mandatory)

[23] Refer 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
	10. The aforementioned committee and the senior management of the REs, including the CISO, shall periodically review instances of cybersecurity incidents/ attacks, if any, domestically and globally, and take steps to strengthen cybersecurity and cyber resilience.	All REs except small-size, Self-certification REs (Mandatory)
	11. The cybersecurity policy shall encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), GoI in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.	All REs which have been identified as CII by NCIIPC (Mandatory)
	12. REs shall incorporate best practices from standards such as ISO 27001, ISO 27002, etc. or their subsequent revisions, if any, from time to time.	All REs except small-size, Self-certification REs
GV.OV: Guidelines		
GV.OV.S4	1. REs shall conduct third-party assessment (for MIIs) and self-assessment (for Qualified REs) of their cyber resilience using CCI and submit corresponding evidences to their submission authority on a periodic[24] basis. CCI and its calculation methodology has been attached at **Annexure-K**. REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance of CCI. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.	MIIs and Qualified REs (Mandatory)
GV.RM: Guidelines		

[24] Refer 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
GV.RM.S1, GV.RM.S2	1. Risk Management a. The design of the cyber risk management framework needs to consider the following (including but not limited to): i. Identification of the cybersecurity risk for the organization ii. Classification of identified and mapped business functions, supporting processes and information assets at risk. iii. Determination of risk appetite for IT and cybersecurity risks. iv. Definition of mitigation measures and controls to reduce the risks. v. Monitoring of the effectiveness of the above-mentioned measures and controls. vi. Evaluation of the effect of major changes and significant operational, technical or cybersecurity incident(s) on the risks. b. REs shall consider using latest version of ISO 27005 as a guidance on design, implementation, and maintenance of information security risk management. c. Risk management strategy of REs shall include (but not limited to) risk assessment, risk analysis, risk mitigation, risk monitoring and review, compliance with relevant laws and regulations, communication of risk management policies to all stakeholders, effective mitigation measures with options for compensatory controls wherever feasible, measures to reduce residual risk and ensuring that the cybersecurity risk tolerance is within acceptable limits. d. REs shall use metrics like (including but not limited to) MTTD, MTTR, MTTC, number of cybersecurity incidents/ intrusion attempts detected and resolved within a specific period, number of false positives and false negatives generated by cybersecurity monitoring tools, number of successful cyber attacks occurred in the past year, and how these numbers are being reduced through continuous refinement of the monitoring process for measuring their cybersecurity maturity level.	All REs except small-size, self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	e. REs shall periodically assess level of employee cybersecurity awareness, for e.g., through phishing test success rate, etc. f. REs shall undertake periodic IT asset management for functions such as number of devices on the network running end-of-life (EOL) software, number of devices no longer receiving security updates, unidentified devices on the internal network, integration of third-party devices and services into the network, etc. Further, IT asset management may also be utilized for process of managing assets' access and permissions, patching cadence, security rating, third-party security rating, number of known vulnerabilities, etc. g. Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all delivery channels.	
GV.RM.S3	1. Comprehensive scenario-based testing shall be done for assessing cybersecurity risks of the RE. A sample list of possible attack scenarios and possibilities for Stock Exchanges have been attached at **Annexure-E**. Other MIIs and REs shall prepare their own attack scenarios as per their business model and assess their risks accordingly.	All REs except small-size, self-certification REs (Mandatory)
GV.SC: Guidelines		
GV.SC.S4	1. Where the systems (IBT, Back office and other customer facing applications, IT infrastructure, etc.) of a RE are managed by third-party service providers and in case the RE does not have direct control over the implementation of any of the guidelines, the RE shall instruct the third-party service providers to adhere to the applicable guidelines in the CSCRF and shall obtain the necessary cyber audit certifications from them to ensure compliance with the framework.	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	2. Where applications (for e.g.: NSE's NEAT, BSE's BOLT etc.) are offered to users over the internet by MIIs , the responsibility of ensuring cyber resilience of such applications resides with the MIIs and not with the users who are using the applications.	MIIs (Mandatory)
	3. The responsibility, accountability and ownership of outsourced activities lies primarily with REs. Therefore, REs shall come up with appropriate monitoring mechanisms through a clearly defined framework to ensure that all the requirements as specified in CSCRF shall be complied with. The periodic[25] reports submitted to SEBI shall highlight the critical activities handled by the third-party service providers and REs shall certify that the above-mentioned requirement is complied with. 4. REs shall conduct background checks and ensure signing of Non-Disclosure Agreement, and cybersecurity compliance for all third-party service providers.	All REs (Mandatory)
GV.SC.S5	1. REs shall obtain SBOM for existing their *critical systems* within 6 months (starting from the date of issuance of CSCRF). 2. REs shall obtain SBOMs for any new *critical systems* software products/ Software-as-a-Service applications (SaaS) at the time of procurement. SBOMs containing information such as all the open source and third-party components present in a codebase, versions of the components used in the codebase, and their patch status, etc. allow security teams to quickly identify any associated security or license risk. 3. MIIs shall include SBOM as part of their empanelment criteria for application software vendors. 4. SBOM shall include (but not limited to) the following:	All REs (Mandatory)

[25] Refer 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
	a. License information b. Name of the supplier c. All primary (top level) components with all their transitive dependencies (including third-party dependencies whether in-house or open-source components) and relationships d. Encryption used e. Cryptographic hash of the components f. Frequency of updates g. Known unknown (where a SBOM does not include a full dependency graph) h. Access control i. Methods for accommodating occasional incidental errors.	
GV.SC.S7	1. Any single third-party service provider, providing services to multiple REs, creates a concentration risk. When such third-party service providers encounter cybersecurity incidents/ attacks, it can led to systemic implications due to high concentration risk. Therefore, REs need to take into account concentration risk while outsourcing multiple critical services to the same third-party service provider. 2. REs shall identify their third-party service providers posing a concentration risk and shall prescribe specific cybersecurity controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk. REs shall also validate that such third-party service providers are meeting their goals of operational resiliency. 3. Stock Exchanges/ Depositories shall take necessary steps to mitigate concentration risk of third-party service providers among Stock Brokers/ Depository Participants.	All REs except small-size, self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	4. SEBI circulars on outsourcing of activities, currently mandated and updated from time to time, shall be complied with by the respective REs. List of currently mandated SEBI circulars on outsourcing of activities has been attached at **Annexure-F**.	
Cyber Resilience goal: ANTICIPATE		
Cybersecurity control: IDENTIFY		
ID.AM: Guidelines		
ID.AM.S1, ID.AM.S4	1. All REs shall identify and classify *critical systems* as defined in this framework based on their sensitivity and criticality for business operations, services and data management. The Board/ Partners/ Proprietor of the REs shall approve the list of *critical systems*. 2. All REs shall maintain an up-to-date inventory of their (including but not limited to) hardware and systems, software, digital assets (such as URLs, domain names, application, APIs, etc.), shared resources (including cloud assets), interfacing systems (internal and external), details of its network resources, connections to its network and data flows. 3. Any additions/ deletions or changes in existing assets shall be reflected in the asset inventory within 3 working days. 4. For conducting criticality assessment of assets, REs shall take the following steps (including but not limited to): a. Maintain a comprehensive asset inventory b. Conduct threat modelling (based on risk assessment) c. Conduct vulnerability assessment 5. REs shall prepare and maintain an up-to-date network architecture diagram at the organisational level including wired and wireless networks.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	6. REs shall put in place configuration management database approach to: a. Understand and inventorise their IT assets - both logical (e.g., data, software) and physical (e.g., hardware). b. Understand which data or systems are most critical for providing critical services as well as any associated interdependencies.	MIIs (Mandatory)
ID.AM.S6	7. All IT assets shall be inventoried in ITSM tool. 8. REs shall integrate cybersecurity considerations into product life cycles.	All REs except small-size, self-certification REs (Mandatory)
ID.RA: Guidelines		
ID.RA.S1, ID.RA.S2	1. REs shall conduct a risk assessment (including post-quantum risks) of the IT environment of their organization on a half-yearly (for MIIs) and yearly (for qualified and mid-size REs) basis to acquire visibility and a reasonably accurate assessment of the overall cybersecurity risk posture. The above-mentioned risk assessment shall be utilized by the RE to develop a quantifiable cybersecurity risk score. 2. REs shall accordingly identify cyber risks[26] that they may face, along with the likelihood of associated threats and their impact on their business, and deploy controls commensurate to their criticality. 3. Risk Assessment shall include (but not limited to): a. Technology stack and solutions used b. Known vulnerabilities c. Dependence on third-party service providers d. Data storage, security and privacy protection	All REs except small-size, self-certification REs (Mandatory)

[26] Refer Definitions section for the Risk definition.

Standards	CSCRF guidelines	Applicability
	e. Threats, likelihoods and associated risks	
ID.RA.S3	1. REs shall engage Dark web monitoring (for brand intelligence, customer protection, etc.), and takedown services as a cyber-defence strategy to check for any brand abuse, data/credentials leak, combating cyber abuse etc. 2. REs shall subscribe to anti-phishing/ anti-rogue app services to mitigate potential phishing or impersonation attacks. 3. REs shall devise SOPs to implement the advisories issued by CERT-In, NCIIPC or any other government agency in their IT environment within a defined timeframe. 4. REs shall have processes in place to manage and incorporate IOAs/ IOCs/ malware alerts/ vulnerability alerts (received from CERT-In or NCIIPC (as applicable) or any other government agencies) in their systems. 5. REs shall be onboarded to CERT-In intelligence platform to receive the advisories for necessary action and implementation.	MIIs, Qualified REs (Mandatory)
	6. MIIs shall get onboarded to NCCC to generate necessary situational awareness of existing and potential cybersecurity threats, and enable timely information sharing for taking proactive, preventive, and protective actions by individual entities.	MIIs (Mandatory)
ID.RA.S4	1. <u>Measures against Phishing websites and attacks</u> a. REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. REs' domains and report the same to CSIRT-Fin/CERT-In for taking appropriate action.	All REs (Mandatory)
	2. Risk assessment of authentication-based solutions shall be implemented to get insights about context behind every login. Further, when a user attempts to sign-in, risk-based	All REs

Standards	CSCRF guidelines	Applicability
	authentication solution shall analyse factors such as device, location, network, sensitivity, etc.	
Cyber Resilience goal: ANTICIPATE		
Cybersecurity control: PROTECT		
PR.AA: Guidelines		
PR.AA.S1, PR.AA.S2, PR.AA.S3, PR.AA.S7, PR.AA.S9	1. <u>Access Controls, Password Policy/ Authentication Mechanism</u> a. No person by virtue of rank or position shall have any intrinsic right to access confidential data applications, system resources or facilities. b. Any access to REs' systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. Access granted to IT systems, applications, databases and networks shall be on a need-to-use basis and based on the principle of least privilege. Such access shall be given for a specific duration and using effective authentication mechanisms. c. User access rights, delegated access and unused tokens, and privileged users' activities shall be reviewed on a periodic basis. d. Access to external cloud services such as Dropbox, google drive, iCloud, OneDrive, etc. shall be given as per RE's policy. e. 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 (atleast 6 months in online mode and rest in archival mode). REs also need to maintain records of users with access to shared accounts. f. Account access lock policies after failure attempts shall be implemented for all accounts.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	g. Existing user accounts and access rights shall be periodically reviewed by the owner of the system in order to detect dormant accounts, accounts with excessive privileges, unknown accounts or any type of discrepancy. h. Proper 'end of life' mechanisms shall be adopted for user management to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn. This includes named user IDs, default user IDs and generic email IDs. i. All *critical systems* accessible over the internet shall have multi-factor security (such as VPNs, Firewall controls, etc.) and MFA. j. MFA shall be enabled for all users and systems that connect using online/ internet facility and also particularly for VPNs, webmail, and accounts that access *critical systems* from non-trusted environments to trusted environments. 2. <u>Network Security Management</u> a. Adequate controls shall be deployed to address virus/ malware/ ransomware attacks on servers and other IT systems. These controls may include host/ network/ application based IPS, customized kernels for Linux, anti-virus and anti-malware software, etc. Anti-virus definition files updates and automatic anti-virus scanning shall be done on a regular basis. b. All REs shall establish baseline standards to facilitate consistent application of security configurations to OS, databases, network devices, enterprise mobile devices, etc. within the IT environment. REs shall also conduct regular enforcement checks to ensure that baseline standards are applied uniformly. c. The LAN and wireless networks within REs' premises shall be secured with proper access controls.	

Standards	CSCRF guidelines	Applicability
	d. REs shall keep total and maximum connections to SMTP server limited.	
	3. Access Controls, Password Policy/ Authentication Mechanism a. PIM solution or PIM process shall be implemented to keep track of privileged access. b. REs shall implement an access policy which addresses strong password controls for users' access to systems, applications, networks and databases, etc. Illustrative examples for this are given in **Annexure-G**. c. REs shall formulate an Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the critical IT infrastructure of REs. d. REs shall deploy controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures shall inter-alia include restricting the number of privileged users, periodic[27] review of privileged users' activities, disallow privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc. 4. Network Security Management a. REs shall apply appropriate network segmentation/ isolation techniques to restrict access to the sensitive information, hosts and services. Segment to segment access shall be based on strong access control policy and principle of least privilege.	All REs except small-size, self-certification REs (Mandatory)

[27] Refer Table 15 in 'CSCRF Compliance, Audit Report Submission, and Timelines' section.

Standards	CSCRF guidelines	Applicability
	b. REs shall install network security devices, such as WAF, proxy servers, IPS, etc. to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources. c. REs shall deploy web and email filters on the network. These devices shall be configured to scan for known bad domains, sources, and addresses, block these before receiving and downloading message and filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses, malicious domains/URLs at the firewall. All emails, attachments, and downloads both on the host and at the mail gateway shall be scanned with a reputable antivirus solution. d. Network devices of REs shall be configured in line with whitelist approach of IPs, ports and services for inbound and outbound communication with proper ACL implementation. e. REs shall implement DNS filtering services to ensure clean DNS traffic is allowed in the environment. DNS security extension for secure communication shall be used. f. Management of critical servers/ applications/ services/ network elements shall be restricted through enterprise identified intranet systems. g. REs shall implement SPF, DMARC, and DKIM for email security. h. Email protection shall include (but not limited to) best practices like strong password protection, MFA, spam filtering, email encryption, secure email gateway, permissible attachments types, etc. i. REs shall block malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/ CERT-In advisories which are published periodically shall be referred for latest malicious domains/ IPs, C&C DNS and links.	

Standards	CSCRF guidelines	Applicability
	j. REs shall maintain an up-to-date and centralised inventory of authorised devices connected to REs' network (within/ outside RE's premises) and authorised devices enabling the REs' network. The REs may consider implementing solutions to automate network discovery and management.	
PR.AA.S1, PR.AA.S2, PR.AA.S3	1. Stock Brokers who are providing algorithmic trading facilities shall take adequate measures to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.	Stock Brokers/ Depository Participants (Mandatory)
PR.AA.S4, PR.AA.S5	1. REs shall follow zero-trust security model in such a way that access (from within or outside REs' network) to their *critical systems* is by default denied by default and allowed only after proper authentication and authorization. 2. Delegated access and unused tokens shall be reviewed and cleaned at least on a quarterly basis.	MIIs and Qualified REs (Mandatory)
PR.AA.S6	1. Effective authentication policy shall be implemented with the defined complexity of the password. 2. All generic user IDs and email IDs which are not in use shall be removed after the use.	All REs (Mandatory)
	3. REs shall implement strong password controls for users' access to systems, applications, networks, databases, etc. Password controls shall include (but not limited to) a change of password upon first login, minimum password length and history, password complexity as well as maximum validity period. 4. The user credential data shall be stored using strong hashing algorithms.	All REs except small-size, self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
PR.AA.S8	1. REs are advised to ensure that all logs sources are being identified and their respective logs are being collected. An indicative list of types of log data to be collected by REs is as follows: system logs, application logs, network logs, database logs, security logs, performance logs, audit trail logs, and event logs. 2. Strong log retention policy shall be implemented as per government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023, and as required by CERT-In, NCIIPC or any other government agency. 3. In order to identify unusual patterns and behaviours, monitoring of all logs of events and incidents shall be done.	All REs (Mandatory)
PR.AA.S10, PR.AA.S11, PR.AA.S12	1. <u>Physical Security</u> a. Physical access to the *critical systems* shall be restricted to a minimum and shall be provided only to authorized officials. Physical access provided to third-party service providers shall be properly supervised by ensuring at the minimum that third-party service providers are accompanied at all times by authorized employees. b. Employees of REs shall be screened before granting access to organizational information and information systems. Physical access to the *critical systems* shall be revoked immediately if the same is no longer required. c. All REs shall ensure that the perimeter of the critical equipment's room, if any, are physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. wherever appropriate. 2. <u>Remote Support Service Security</u>	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	a. As many OEMs and their service partners as well as System Integrators provide remote support services to organisations, REs shall ensure that these services are well-governed, controlled, logged and an oversight is maintained on all the activities done by remote support service providers. The above shall be complemented by regular monitoring and audit to ensure compliance of the defined policies for privileged users and remote access. b. REs shall ensure secure usage of RDP in IT systems. Further, it shall be implemented strictly on a need-to-use basis, and it must employ MFA. Remote access, if necessary, shall be given to authorised personnel from whitelisted IPs for a predefined time period, and with a provision to log all activities. c. Employees and third-party service providers who may be given authorized access to the *critical systems*, networks and other IT resources of REs shall be subject to stringent supervision, monitoring and access restrictions.	
	d. Environmental controls (temperature, water, smoke, etc.), service availability alerts (power supply, servers, etc.), access logs, etc. shall be monitored.	All REs except small, self-certification REs (Mandatory)
PR.AA.S13, PR.AA.S14	1. REs shall formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data. 2. REs shall frame suitable policies for disposal of storage media and systems. The critical data/ information on such devices and systems shall be removed by using methods such as wiping/ cleaning/ overwrite, degauss/ crypto shredding/ physical destruction as applicable.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
PR.AA.S15	1. Endpoint security a. Solutions like EPP, EDR, XDR, anti-malware software etc. shall be implemented to detect threats and attacks on endpoint devices, and to enable immediate response to such threats and attacks. Further, REs shall ensure that signatures are updated on all IT systems. b. Solutions like IPS/ NG-IPS shall be used to continuously monitor the organizations' network for malicious activities. c. PowerShell and local admin rights shall be disabled by default on endpoint machines and shall be used only for a specific purpose and for a limited time. 2. Guidance on usage of Active Directory (AD) servers a. REs shall regularly review the AD to locate and close existing backdoors such as compromised service accounts, which often have administrative privileges and are a potential target of attacks. b. REs shall undertake the penetration testing activity for known AD Domain Controller abuse attacks. Weaknesses shall be remediated on topmost priority. 3. Restricted use of removable media and electronic devices a. REs shall define and implement policy for restriction and secure use of removable media (such as USB, external hard disks, etc.) and electronic devices (such as laptops, mobile devices, etc.). REs shall ensure secure erasure of data so that no data is in recoverable form on such media and electronic devices after use.	All REs except small-size, self-certification REs (Mandatory)
	4. Secure Domain Controllers (DCs)	MIIs (Mandatory)

Standards	CSCRF guidelines	Applicability
	Threat actors often target and use DCs as a staging point to spread ransomware network-wide. a. REs shall ensure that DCs are patched as and when patch is released and it must be reviewed on a quarterly basis to ensure the implementation of the same. b. REs shall ensure that no unnecessary software is installed on DCs, as these can be leveraged to run arbitrary code on the system. c. REs shall ensure that access to DCs should be restricted to the Administrators group. Users within this group shall be limited and have separate accounts used for day-to-day operations with non-administrative permissions. d. REs shall ensure that DC host firewalls are configured to prevent direct internet access.	
PR.AA.S16, PR.AA.S17	1. <u>API security</u> a. API security protects against vulnerabilities and misconfigurations in the APIs and prevents their misuse. Thus, effective API security strategies like rate limiting, throttling, etc. shall be used while developing APIs to prevent overuse or abuse. If APIs have been provided by MIIs and consumed by REs then onus of ensuring API security shall be on MIIs. MIIs shall have API security solutions in place for securing services and data transmitted through APIs. b. Proper access management, and effective authentication and authorization shall be done to ensure that only the desired entities have access to the APIs. c. OWASP documentation for developing APIs shall be followed and OWASP top 10 API security risks shall be mitigated. d. Connecting to entities via APIs shall be strictly on a whitelist-based approach.	All REs except small-size, Self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	2. Mobile Application Security a. The mobile application shall perform root detection and root cloaking detection. The application shall not work on emulators or virtual devices. b. REs shall explore the feasibility of implementing a code that checks if the device is rooted/ jailbroken prior to the installation of the mobile application and disallow the mobile application to install/ function if the phone is rooted/ jailbroken. c. Device Policy enforcement such as detection of developer option, USB debugging, Mock Location, time settings manipulation, etc. shall be configured. d. Mobile application shall check new network connections or connections for unsecured networks like VPN connection, proxy and unsecured Wi-Fi connections. e. Mobile application shall have anti-malware capabilities covering application spoofing, RAT, screen mirroring, overlay malwares, key loggers, tap jacking, etc. f. Controls to prevent reverse engineering and application tampering shall be implemented in the mobile applications. These controls shall also validate the signature during runtime for authenticity of the application. g. Mobile application shall perform checksum validation and the checksum of applications shall be published in public domain. h. Mobile application shall identify the presence of active remote access, screen mirroring, active voice call, alert users, etc. to prevent online frauds. i. Mobile application shall require re-authentication whenever the device of the application remains unused for a designated period and also each time the investor/ user launches the application. j. Mobile application shall not store/ retain sensitive personal/ investor authentication information such as user IDs, passwords, keys, hashes, hard coded reference, etc.	

Standards	CSCRF guidelines	Applicability
	on the device and the application shall also securely wipe out any sensitive investor/ user information from memory when the investor/ user exits the application. k. Mobile application shall be secured against common vulnerabilities such as SQL injection, etc. l. REs shall ensure that the usage of raw SQL queries in mobile application to fetch or update data from databases is avoided. Additionally, sensitive information shall be written to the database in an encrypted form.	
	m. Mobile application shall implement device-binding solution to create a unique digital identity based on device, mobile number and SIM. n. OWASP – MASVS shall be referred for implementing mobile application security and other protection measures. o. REs shall consider implementing measures such as installing a "containerized" app on mobile/ smart phones for exclusive business use that is encrypted and separated from other smartphone data/ applications; implement measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.	All REs except small-size, self-certification REs
	3. <u>Guidelines for Application Security and Emerging Technologies</u> REs shall prepare SOPs for open source application security and concerns from emerging technologies like Generative AI security.	MIIs and Qualified REs
PR.AT: Guidelines		
PR.AT.S1, PR.AT.S2	1. REs shall work on building awareness of cybersecurity, cyber resilience, and system hygiene among employees (with a focus on employees from non-technical disciplines). 2. REs shall ensure that their employees are aware of potential risks including social engineering attacks, phishing, etc.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	3. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, shall be established as an essential pillar of defence. Additionally, the advisories issues by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness. 4. REs shall conduct periodic training programs to enhance knowledge of IT/ cybersecurity policy and standards among the employees incorporating up-to-date cybersecurity threats. Wherever possible, this shall be extended to outsourced staff, third-party service providers, etc. 5. The training programs shall be reviewed and updated to ensure that the contents of the program remain current and relevant.	
PR.AT.S3	1. REs shall mention/ incorporate a section on the mobile and web application clearly specifying the process and procedure (with forms/ contact information, etc.) to lodge customer/ investor grievances with respect to technology related issues and cybersecurity. A mechanism to keep this information periodically updated shall also be put in place. The reporting facility on the application shall provide an option for registering a grievance. Customers/ investors dispute handling, reporting and resolution procedures, including the expected timelines for the response should be clearly defined. 2. REs shall provide access to mobile and web applications to a customer only at her/ his option based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions. 3. REs shall provide a mechanism on their mobile and web application for their customers/ investors with necessary authentication to identify/ mark a transaction as fraudulent for	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	seamless and immediate notification to his entities. On such notification by the customer/investor, they may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty's entities; vice-versa have mechanism to receive such fraudulent transactions reported from other entities. 4. Improve and maintain customer/ investor awareness and education with regard to cybersecurity risks. 5. Encourage customers/investors to report phishing mails/ phishing sites and on such reporting take effective remedial action. 6. Educate the customers/investors on the downside risk of sharing their login credentials/ passwords/ OTP etc. to any third-party and the consequences thereof.	
PR.DS: Guidelines		
PR.DS.S1, PR.DS.S2, PR.DS.S3	1. <u>Data and Storage Devices security</u> a. Data shall be encrypted in motion, at rest and in-use by using strong encryption methods. Data-in-use encryption shall be applicable for cloud deployment (refer **Annexure-J**). Layering of Full-disk Encryption (FDE) along with File-based Encryption (FBE) shall be used wherever possible. REs shall use industry standard, strong encryption algorithms (e.g., RSA, AES, etc.) wherever encryption is implemented. Illustrative measures in this regard are given in **Annexure-H** and **Annexure-I**. b. REs shall deploy Data Loss Prevention (DLP) solutions/ processes. c. REs shall implement measures to prevent unauthorized access, copying, transmission of data/ information held in contractual or fiduciary capacity. It shall be ensured that confidentiality of information is not compromised during the process of	All REs except small-size, self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	exchanging and transferring information with external parties. Illustrative measures to ensure security during transportation of data over the internet are given in **Annexure-I**. d. The information security policy shall also cover use of devices such as mobile phones, photocopiers, scanners, etc., which can be used for capturing and transmission of sensitive data within their IT infrastructure. For instance, defining access policies for personnel, network connectivity for such devices, etc. e. REs shall allow only authorized data storage device within their IT infrastructure through appropriate validation processes.	
	2. <u>Application Security in Customer Facing Applications:</u> a. Application security for Customer facing applications offered over the Internet such as IBTs (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by REs to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. An illustrative list of measures for ensuring security in such applications is provided in **Annexure-G**.	All REs except self-certification REs (Mandatory)
	1. REs shall implement suitable mechanisms, including generation of appropriate alerts, to monitor capacity utilisation on a real-time basis and shall proactively address issues pertaining to their capacity needs. 2. For capacity planning and monitoring, REs shall comply with circulars/ guidelines on capacity planning issued by SEBI (and updated from time to time).	All REs except self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	1. REs shall keep the *Regulatory Data* available and easily accessible in legible and usable form, within the legal boundaries of India. However, for the investors whose country of incorporation is outside India, the REs shall keep the original data, available and easily accessible in legible and usable form, within the legal boundaries of India. Further, if the *Regulatory Data* retained within India is not in readable form, the REs must maintain an application/system to read/ analyse the retained data. 2. The *IT and Cybersecurity Data* which is sent to/ consumed by global/ international SOC of the REs and SaaS based cybersecurity solutions have been exempted from being maintained within the legal boundaries of India. For above mentioned SaaS based cybersecurity solutions and SOC offerings utilized by REs where the data is not processed/stored within the legal boundaries of India, such data shall be classified, assessed and periodically reviewed (at least once in a year) by the respective *IT Committee for REs* or equivalent body of the RE. Additionally, such *IT and Cybersecurity Data* shall be approved by the Board/ Partners/ Proprietor annually. Further, such data shall be made available to SEBI/ CERT-In/ any other government agency whenever required within a reasonable time not exceeding 48 hours from the time of request. 3. While doing data classification, REs shall adhere to data security standards and guidelines and other government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by SEBI/ GoI such as IT Act 2000, Digital Personal Data Protection Act (DPDP) 2023 or any other law/ circular/ regulation as and when issued.	All REs (Mandatory)
PR.DS.S4	1. REs shall enforce effective data protection, backup, and recovery measures. 2. REs shall block administrative rights on end-user workstations/ PCs/ laptops by default and provide access rights on need basis as per the established process and approvals and for specific duration for which it is required.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	3. Security controls for mobile and web applications shall focus on how these applications handle, store, and protect PII and other business related data. 4. Web and mobile applications shall not store sensitive information in HTML hidden fields, cookies, or any other client-side storage to avoid any compromise in the integrity of the data. 5. REs shall renew their digital certificates used in IT systems well in time. 6. REs shall implement measures to control usage of VBA/macros in office documents, control permissible attachment types in email systems. 7. REs shall have a documented data migration policy specifying SOPs and processes for data migration while ensuring data integrity, completeness and consistency.	
PR.DS.S5	1. For the development of all software/ applications and feature enhancements, there shall be separate production and non-production environments. 2. After development and/ or feature enhancement, SIT shall be done to ensure that the complete software/ application is working as required. 3. During the development phase of any software/application to be used by the REs or customers of REs, it shall be ensured that vulnerabilities identified by best practices baselines such as OWASP, top 25 software security vulnerabilities identified by SANS, etc. are addressed. It is recommended that REs should adopt methodologies like DevSecOps for secure development of their applications/ software.	MIIs and Qualified REs (Mandatory)
PR.DS.S6	1. REs shall obtain the source codes for all critical applications from their third-party service providers. Where obtaining of the source code is not possible, REs shall put in place a source code escrow arrangement or other equivalent arrangements to adequately mitigate the risk of default by the third-party service provider. REs shall ensure that all	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	product updates and patches/ fixes are included in the source code escrow arrangement. 2. For all the software and applications, where vulnerabilities will be identified at a later date, REs shall ensure that the vulnerabilities shall be mitigated in a time bound manner. REs shall also stipulate timelines in their SLA with their third-party service providers for the timely compliance and closure of identified vulnerabilities. 3. REs shall put in place appropriate third-party service providers (including software vendors) risk assessment process and controls proportionate to their criticality/ risk in order to manage supply chain risks effectively. 4. REs shall ensure that maintenance and necessary support for applications/ software is provided by the third-party service providers (including software vendors) and the same is enforced through a formal agreement.	
PR.IP: Guidelines		
PR.IP.S1	1. REs shall ensure that IT, OT and IS infrastructure is 'secure by design', 'secure by engineering/ implementation' and the infrastructure has appropriate elements to ensure 'secure IT operations'. 2. For implementation of principle of least functionality, measures such as configuring only essential capabilities by disabling unnecessary and/or unsecured functions, ports, protocols, services, etc. within an information systems shall be implemented.	All REs
	3. REs shall use application directory whitelisting on all assets to ensure that only authorized software are run and all unauthorized software are blocked from installation/ execution.	All REs except small-size, self-certification REs (Mandatory)
	1. Hardening of Hardware and Software	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	a. REs shall deploy only hardened and vetted hardware/ software. During the hardening process, REs shall, inter-alia, ensure that default usernames and passwords are replaced with non-standard usernames and strong passwords and all unnecessary services are removed or disabled in software/ system. b. Hardening of OS shall be done to protect servers'/ endpoints' OS, and minimize attack surface and exposure to threats. c. For running services, non-default ports shall be used wherever applicable. Open ports on networks and systems, which are not in use or can be potentially used for exploitation of data, shall be blocked. All open ports shall be monitored and appropriate measures shall be taken to secure them. d. Practice of whitelisting of ports based (at firewall level) on business usage shall be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted shall be blocked by default. e. REs shall restrict execution of "PowerShell" and "wscript" in their environment, if not required. Additionally, REs shall also ensure installation and use of latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis. f. REs shall utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communications among endpoints wherever possible to limit lateral movement as well as other attack activities.	
PR.IP.S3	1. The change management process shall be part of all agreements with third-party service providers to ensure that changes to the system are implemented in a controlled and coordinated manner.	All REs except small-size, self-certification REs

Standards	CSCRF guidelines	Applicability
	2. Change Management process shall include (but not limited to) submission, planning (impact analysis, rollout plan), approval, and implementation, review (post-implementation), closure, etc. 3. REs shall have a clearly defined framework for change management including requirements justifying exception(s), duration of exception(s), process of granting exception(s), and authority for approving and for periodic review of exception(s) given.	
PR.IP.S4, PR.IP.S6	3. <u>Secure Software Development Life Cycle (SSDLC)</u> a. All REs shall ensure that regression testing is undertaken before new or modified systems are implemented. The scope of tests shall cover business logic, security controls and system performance under various stress-load scenarios, and recovery conditions. b. For any production release, vulnerability assessment shall be undertaken. For all *major release*, VAPT shall be conducted by the REs to assess the risk and vulnerabilities generated from recent additions/ modifications in applications/ software.	All REs except small-size, self-certification REs (Mandatory)
	4. <u>Secure Software Development Cycle (SSDLC)</u> a. REs shall prepare business requirement document with clear mentioning of security requirements, session management, audit trail, logging, data integrity, security event tracking, exception handling, etc. b. For secure rollout of software and applications, threat modelling and application security testing shall be conducted during development. c. REs shall refer to standards, security guidelines for application security and other protection measures given by OWASP (for e.g. OWASP-ASVS).	All REs

Standards	CSCRF guidelines	Applicability
	d. REs shall adopt the principle of defence-in-depth to provide a layered security mechanism. e. Before introducing new technologies for *critical systems*, REs shall ensure that IT/ security team has assessed evolving security concerns and achieved fair level of maturity with such technologies before incorporating them into IT infrastructure.	
PR.IP.S14	1. <u>Periodic Audit</u> a. REs shall engage only CERT-In empanelled IS auditing organizations for conducting external audits including cyber audit to audit the implementation of all standards mentioned in this framework. b. A CERT-In empanelled IS auditing organisation can audit the RE for a maximum period of three consecutive years. Subsequently, the said IS auditing organisation shall be eligible for auditing the RE again only after a cooling off period of two years. c. The details of periodicity, timeline and report submission for cyber audit by REs have been provided in the *'CSCRF Compliance, Audit Report Submission, and Timelines'* section. d. Along with the cyber audit reports, henceforth, all REs shall also submit a declaration from the Managing Director (MD)/ Chief Executive Officer (CEO) as mentioned in **Annexure-B**. e. To ensure that all the open vulnerabilities in the IT assets of REs have been fixed, revalidation VAPT and cyber audit shall also be done in a time bound manner. f. Audit Management process of the REs shall include (but not limited to) audit program/ calendar, planning, preparation, delivery, evaluation, reporting, and follow-up, etc.	All REs except self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	g. For conducting audits, CERT-In '*IT Security Auditing Guidelines for Auditee Organizations'* may be followed by REs. Additionally, CERT-In *'Guidelines for CERT-In Empanelled IS Auditing Organizations'* (attached at **Annexure-D)** may be mandated for empanelled IS auditing organizations. h. Due diligence with respect to the audit process and the tools used for such audits shall be undertaken by REs to ensure competence and effectiveness of audits.	
	i. REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance with CSCRF. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.	MIIs and Qualified REs (Mandatory)
PR.IP.S15	1. All the categories of software solutions/ applications/ products for *critical systems* used by REs shall mandatorily pass-through the following tests/ audits and compliances: a. Application security testing: i. Dynamic Application Security Testing (DAST) for scanning software applications in real-time against leading vulnerability sources, such as OWASP Top 10, SANS Top 25 CWE, etc. to find security flaws or open vulnerabilities. ii. Static Application Security Testing (SAST) for analyzing program source code to identify security vulnerabilities such as SQL injection, buffer overflows, XML external entity (XXE) attacks, OWASP Top 10 security risks, etc. b. Functional audit c. VAPT after every *major release* of the application/software d. All *critical systems* logs shall be integrated with RE's SOC. e. Audit of firewall configuration, WAF configuration, token configuration and channel identification shall be done.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	f. Software bill of material (SBOM) g. Requirement Traceability Matrix 2. Tests/ audits stated above at point 1 (a-b) shall be limited to cybersecurity aspects. Application security testing shall also include API security and API discovery. Scope of functional audit shall cover data integrity, report integrity, and transaction integrity, etc. 3. With respect to empanelled COTS used by Stock Brokers and Depository Participants: a. Before empaneling any COTS solutions for supplying software/ products to their respective stock brokers and depository participants, Stock Exchanges and Depositories shall conduct tests/ audits stated above at point 1 (a-b) through STQC. b. The Stock Exchanges and Depositories shall prepare a SOP for inclusion of tests/ audits in their vendor empanelment process for COTS solutions. c. The empanelment shall be approved by the Stock Exchanges and Depositories only after receipt of compliance reports from STQC and VAPT report from the COTS vendor. 4. Customized COTS: a. REs shall ensure that the compliance with tests/ audits stated above at point 1 (a-d) by CERT-In empanelled IS auditing organization for any customized COTS. 5. Inhouse developed software: a. REs shall ensure compliance with aforementioned point 1 is submitted by CERT-In empanelled IS auditing organization. 6. Software services in form of SaaS/ hosted services used by REs: i. REs shall be required to submit compliance with the technical specification mentioned in hosted services definition for the SaaS/ hosted services used by them.	

Standards	CSCRF guidelines	Applicability
	ii. REs shall also submit compliance with adoption of hosted services and SaaS as per the various functions of CSCRF including Governance, Identify, Protect, Detect, Respond, and Recover.	
PR.IP.S16	1. ISO 27001 certification shall be mandatory for REs as it provides essential security standards with respect to ISMS. The scope for ISO 27001 certification shall include (but not limited to) PDC site, DR site, NDR site, SOC, and Colocation facility.	MIIs and qualified REs (Mandatory)
PR.IP.S17	1. REs shall follow the latest version of CIS Controls or equivalent standards which are prioritized set of safeguards and actions for cyber defence and provide specific and actionable ways to mitigate prevalent cybersecurity incidents/ attacks.	MIIs and qualified REs (Mandatory)
PR.MA: Guidelines		
PR.MA.S2	1. REs shall ensure proper remote access policy framework incorporating the specific requirements of accessing the enterprise resources (located in the data centre) securely from home using internet connection. 2. REs shall ensure that only trusted client machines shall be permitted to access enterprise IT resources remotely. REs shall put in place appropriate security control measures such as (including but not limited to) host integrity check, binding of MAC address of the device with the IP address, etc. for remote access and telecommuting. 3. REs shall ensure that appropriate risk mitigation mechanisms are put in place whenever remote access of data centre resources is permitted for third-party service providers. 4. REs shall ensure that remote access shall be monitored continuously for any abnormal/ unauthorized access, and appropriate alerts and alarms shall be generated to address this breach before any damage is done.	All REs except small-size, self-certification REs (Mandatory)

Standards	CSCRF guidelines	Applicability
PR.MA.S3	1. REs shall establish and ensure that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches shall be established to apply them in a timely manner. 2. All operating systems and applications shall be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities, and where patches are not available, virtual patching may be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches shall be sourced only from the authorized sites of the OEM. 3. REs shall perform comprehensive and rigorous testing of security patches and updates, wherever possible, before deployment into the production environment so as to ensure that application of patches does not impact other systems. 4. All patches shall be tested first in non-production environment which shall be identical to the production environment. 5. Hardware and software of *critical systems* shall be replaced before they reach End-of-Life/End-of-Support. 6. Compensatory controls like virtual patching shall be implemented for legacy systems for a maximum period of 6 months. Further, the constraints due to which virtual patching is done shall be legitimate and documented. 7. Procurement of hardware/software shall be aligned with technology refresh policy of the REs.	All REs (Mandatory)
	8. REs shall establish a patch management policy to ensure that all applicable patches (at both PDC and DR Site are identified, assessed, tested and applied to all IT	MIIs and Qualified REs

<table>
<tr><th>Standards</th><th>CSCRF guidelines</th><th>Applicability</th></tr>
<tr><td></td><td>systems/applications in a timely manner. The policy shall be approved by IT Committee for REs. Additionally, the above-mentioned policy on patch management shall be reviewed by IT Committee for REs atleast on an annual basis.
9. REs shall ensure that post application of any patch/ update, the resources deployed are adequate enough to deliver the expected performance.
10. REs shall also establish processes for tracking patch compliance across all IT systems/ applications and reporting the same to their respective IT Committee for REs on a quarterly basis.
11. Based on the criticality of the patches, REs shall ensure that patches are implemented at both PDC and DR site within the upper/ maximum time limit as defined below. However, for emergency patching, patches shall be deployed within timelines as stipulated by the OEMs.

<table>
<tr><th>S. No.</th><th>Criticality of Patch</th><th>Upper/ maximum Timeline</th></tr>
<tr><td>1</td><td>High</td><td>1 week</td></tr>
<tr><td>2</td><td>Moderate</td><td>2 weeks</td></tr>
<tr><td>3</td><td>Low</td><td>1 month</td></tr>
</table>
</td><td>(Mandatory)</td></tr>
<tr><td colspan="3">Cyber Resilience goal: ANTICIPATE</td></tr>
<tr><td colspan="3">Cybersecurity control: DETECT</td></tr>
<tr><td colspan="3">DE.CM: Guidelines</td></tr>
<tr><td>DE.CM.S1,
DE.CM.S2,</td><td>1. Security Continuous Monitoring</td><td>All REs
(Mandatory)</td></tr>
</table>

Standards	CSCRF guidelines	Applicability
DE.CM.S3	a. REs shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events/ alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying and transmission of data/ information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies. b. Suitable alerts shall be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions. c. To enhance the security monitoring, REs (except client-based stock brokers having less than 100 clients) are mandated to employ SOC services for their systems. REs may choose any of the following models to use SOC services: i. RE's own SOC/ group SOC ii. Market SOC implemented mandatorily by NSE, BSE and optionally by NSDL and/ or CDSL iii. Any other third party managed SOC d. Small-Size and Self-certification category REs are mandated to be on-boarded on above-mentioned Market SOC.	
	2. <u>Functional efficacy of SOC</u> a. REs shall measure functional efficacy of their SOC using the quantifiable method given in **Annexure-N**. b. REs shall review the functional efficacy of SOC on a half-yearly basis.	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	c. REs shall deploy solutions such as BAS, CART, decoy, vulnerability management, etc. to enhance their cybersecurity posture.	
	d. Those REs who are utilizing third-party managed SOC services or market SOC shall obtain SOC efficacy report (using the quantifiable method given in **Annexure-N**) from their SOC provider on a yearly basis.	All REs having third-party managed SOC or market SOC (mandatory)
	3. MIIs shall have a cybersecurity Operations Centre (C-SOC) that would be a 24×7×365 set-up manned by dedicated security analysts to identify, respond, recover and protect from cybersecurity incidents[28]. The C-SOC for MIIs shall function in accordance with SEBI circular CIR/MRD/CSC/148/2018 dated December 07, 2018 which has been attached at **Annexure-M**.	MIIs (Mandatory)
DE.CM.S4	1. The use of IT assets/ resources shall be monitored, tuned and projections shall be made for future capacity requirements to ensure the required system performance for meeting the business objectives. 2. To ensure high resilience, high availability and timely detection of attacks on systems and networks, REs shall implement suitable mechanisms to monitor capacity utilization of its *critical systems* and networks. 3. Capacity management shall comprise of three primary types; Data storage capacity – (e.g. in database systems, file storage areas, etc.); Processing power capacity – (e.g. adequate computational power to ensure timely processing operations); and	All REs except small-size, Self-certification REs (Mandatory)

[28] Refer SEBI circular CIR/MRD/CSC/148/2018 dated December 07, 2018.

Standards	CSCRF guidelines	Applicability
	Communications capacity – (“bandwidth” to ensure communications are made in a timely manner). 4. Capacity management shall be; a. Pro-active – for example, using capacity considerations as part of change management; b. Reactive – e.g. triggers and alerts for when capacity usage is reaching a critical threshold so that timely increments (temporary or permanent) can be made.	
DE.CM.S5	1. The details of periodicity, timeline and report submission for cyber audit by REs have been provided in the *‘CSCRF Compliance, Audit Report Submission, and Timelines’* section. 2. REs shall regularly conduct cybersecurity audit and VAPT with scope as mentioned in CSCRF in order to detect vulnerabilities in the IT environment. Further, REs shall conduct in-depth evaluation of the security posture of the system through simulations of actual attacks. An indicative (but not exhaustive and limited to) VAPT scope has been attached at **Annexure-L**. 3. The assets under these audits shall include (but not limited to) all *critical systems*, infrastructure components (like networking systems, security devices, load balancers, servers, databases, applications, remote access points, systems accessible through WAN, LAN as well as with Public IP’s, websites, etc.), and other IT systems pertaining to the operations of REs. 4. REs shall perform VAPT prior to the commissioning of new systems, especially those which are part of *critical systems* or connected to *critical systems*.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	5. Revalidation of VAPT post closure of observations shall be done in a time bound manner to ensure that all the open vulnerabilities have been fixed.	
	6. In case of vulnerabilities being discovered in COTS (used for core business) or empanelled applications, REs shall report them to the vendors and the designated stock exchanges and/ or depositories in a timely manner.	Stock Brokers/ Depository Participants falling under Qualified REs and Mid-size REs (Mandatory)
DE.DP: Guidelines		
DE.DP.S4	1. REs shall conduct red teaming exercises as part of their cybersecurity framework on a half-yearly basis through use of red/ blue teams. 2. CART solution shall be deployed for continuous, automated process of testing the security of the systems, and achieving greater visibility on attack surfaces. 3. For red teaming exercise, a red team may consist of REs employees and/ or outside experts. Additionally, the red team shall be independent of the function being tested. 4. The results of the red teaming exercise shall be placed before *IT Committee for REs* and Governing board. The lessons learned from conducting such red team exercises shall be shared with SEBI within 3 months after completion of the exercise. Status of the remediation of the observation found during the red team exercise shall be monitored by *IT Committee for REs*.	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
DE.DP.S5	1. REs shall proactively search for hidden and undetected cyber threats in their network. 2. Threat hunting by leveraging threat intelligence, IOCs, IOAs, etc. shall be conducted on a quarterly basis.	MIIs and Qualified REs (Mandatory)
Cyber Resilience goal: WITHSTAND & CONTAIN		
Cybersecurity control: RESPOND		
RS.MA: Guidelines		
RS.MA.S1	1. All REs shall formulate an up-to-date CCMP in line with national CCMP of CERT-In. 2. CCMP shall be approved by Board/ Partners/ Proprietor of REs. 3. Incident Response Management a. All REs shall develop an Incident Response Management Plan as part of their CCMP. b. The response plan shall define responsibilities and actions to be performed by its employees and support/ outsourced staff in the event of a cyber-attack or cybersecurity incident. c. REs shall have a SOP for handling cybersecurity incident response and recovery for the various cybersecurity attacks. d. MIIs shall have a SOP for cybersecurity incidents reported to them by the REs under their supervision. e. SOP for reporting of cybersecurity incidents to SEBI is attached at **Annexure-O**. The same shall be adhered to.	All REs (Mandatory)
RS.MA.S2	1. In order to optimize the REs' ability to respond in a timely and appropriate manner, REs shall: a. Create cybersecurity awareness,	All REs except small-size, self-certification REs

Standards	CSCRF guidelines	Applicability
	b. Provide cybersecurity training to the relevant teams, c. Develop/ hire people with appropriate skill-sets, d. Prepare cyber playbooks, e. Create knowledge database for all known adverse conditions and attacks	
RS.MA.S5	1. REs shall collaborate with Cyber Swachhta Kendra (CSK) operated by CERT-In to trace bots and vulnerable service(s) running on their public IP addresses, and receive alerts regarding the same. The alerts received from CSK shall be closed in a time-bound manner. Observations (from CSK) which require a longer time to close shall be put up to the *IT Committee for REs* for their guidance and appropriate mitigation/ closure.	MIIs and Qualified REs (Mandatory)
RS.CO: Guidelines		
RS.CO.S1, RS.CO.S2, RS.CO.S3	1. Any cyber-attack, cybersecurity incident and/ or breach falling under CERT-In Cybersecurity directions[29] shall be notified to SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. This information shall be shared with SEBI through the ***mkt_incidents@sebi.gov.in*** within 6 hours. However, necessary details of the incidents shall be reported on SEBI Incident Reporting Portal within 24 hours. Stock Brokers/ Depository Participants shall also report the incidents to Stock Exchanges/ Depositories along with SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. All other cybersecurity incident(s) shall be reported to SEBI, CERT-In and NCIIPC (as applicable) within 24 hours. 2. REs shall share Threat Intelligence data that is collected, processed, and analysed to gain insights into the motives and behaviour (of the threat actor), target, attack pattern, etc. on SEBI Incident Reporting portal.	All REs (Mandatory)

[29] Refer Q 30 in CERT-In Cybersecurity directions: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

Standards	CSCRF guidelines	Applicability
	3. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the REs, whose systems have been identified as "Protected system" by NCIIPC shall also report the incident to NCIIPC. 4. The quarterly reports containing information on cyber-attacks, threats, cybersecurity incidents and breaches experienced by REs and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities, threats that may be useful for other REs and SEBI, shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year. 5. Such details, which are deemed useful for sharing with other REs, in a masked manner, shall be shared using mechanism to be specified by SEBI from time to time. While sharing the above-mentioned sensitive information, TLP may be followed with four levels of sensitivity: white, green, amber, or red. 6. During the processing of reported incidents by SEBI, REs shall provide regular reports (such as RCA, forensic analysis report, etc.) on the progress of the incident analysis.	
RS.CO.S2	1. *IT Committee for REs* shall discuss response plans, coordination with stakeholders for consistency in response actions, information sharing for better awareness, etc. 2. For the purpose of coordinating incident response, REs shall regularly update the contact details of service providers, intermediaries, and other stakeholders. 3. If the cyber-attack is of high impact[30] and has a broad reach, the RE shall give a press release which shall include (but not limited to) a brief of the incident, actions taken to	MIIs and Qualified REs (Mandatory)

[30] REs shall decide the impact of cyber-attack.

Standards	CSCRF guidelines	Applicability
	recover, normal operation resumption status (once achieved), etc. and inform all the affected customers/ stakeholders. 4. If the cyber-attack is of low impact[31] and has a narrow/low reach, the REs shall inform all the affected customers/ stakeholders.	
	5. REs shall notify the customer/ investor, through alternate communication channels, of all transactions including buy/ sell, payment or fund transfer above a specified value determined by the customer/ investor.	All REs (Mandatory)
RS.AN: Guidelines		
RS.AN.S1, RS.AN.S2, RS.AN.S3	1. Alerts generated from monitoring and detection systems shall be suitably investigated by the REs in order to determine activities that are to be performed to prevent spread of cybersecurity incidents/ attacks or breaches, mitigate their effects and resolve the incidents. 2. Data collection: REs shall collect and preserve data related to the incident, such as system logs, network traffic, and forensic images of affected systems. 3. Incident Analysis: REs shall analyse the data to understand the scope, cause, and impact of the incident, including how the incident occurred, what systems and data were affected, who was responsible, etc. 4. Evidence Preservation: REs shall preserve evidence related to the incident, including digital artefacts, network captures, and memory dumps, in a secure and forensically sound manner.	All REs (Mandatory)

[31] REs shall decide the impact of cyber-attack.

Standards	CSCRF guidelines	Applicability
RS.AN.S4, RS.AN.S5	1. Root Cause Analysis: REs shall perform a root cause analysis (RCA) to identify the specific control that has failed, underlying cause of the incident and the potential areas of improvement. 2. Forensic: Forensic analysis (as appropriate) shall be undertaken by the REs. 3. Any incident of loss or destruction of data or systems shall be thoroughly analysed and lessons learned from such incidents shall be incorporated to strengthen the security mechanisms and improve the recovery planning and processes. 4. Reporting: REs shall create a detailed incident report that includes information on the scope, cause, and impact of the incident, as well as recommendations for improving incident response and recovery capabilities. 5. REs shall conduct a compromise assessment through CERT-In empanelled IS auditing organizations.	All REs (Mandatory)
RS.IM: Guidelines		
RS.IM.S1	1. REs shall periodically[32] review and update their contingency plan, COOP, training exercises, and incident response and recovery plans (including CCMP) to incorporate lessons learned, and strengthen their response capabilities in the event of a future incident/ attack.	All REs except self-certification REs (Mandatory)
	2. Post occurrence of cybersecurity incident (if any), REs shall update their response and recovery plan (including CCMP) to improve their cyber resilience and incorporate the learnings from the cybersecurity incident.	All REs (Mandatory)

[32] Half-yearly for MIIs and Qualified REs. Once in two years for Mid-size and small-size REs.

Standards	CSCRF guidelines	Applicability
RS.IM.S2	3. The updates and changes in the contingency plan, COOP, training exercises, and incident response and recovery plan shall be communicated and approved by the Board/ Partners/ Proprietor.	All REs
Cyber Resilience goal: RECOVER		
Cybersecurity control: RECOVER		
RC.RP: Guidelines		
RC.RP.S1	1. The response and recovery plans of the REs shall include scenario-based classifications. REs shall build their own response and recovery plan as per their business model and include the same in their CCMP. 2. The response and recovery plan of the REs shall have plans for the timely restoration of systems affected by incidents of cybersecurity incidents/ attacks or breaches (for instance, offering alternate services or systems to customers). Tests shall be designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. These tests shall include all stakeholders such as critical service providers, vendors, other linked REs, etc. 3. An indicative (but not exhaustive and limited to) recovery plan to be followed by the REs has been attached at **Annexure-C**.	All REs (Mandatory)
	4. REs shall maintain regularly updated *'golden images'* of *critical systems* at offsite location for rebuilding the systems (whenever required). This entails maintaining images "templates" that include a preconfigured operating system (OS), configuration setting backup and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.	MIIs and Qualified REs (Mandatory)

Standards	CSCRF guidelines	Applicability
	5. REs shall explore the possibility of retaining spare hardware in an isolated environment to rebuild systems in an event that starting REs' operations from PDC and/ or DRS is not feasible. The REs shall also try to keep spare hardware in ready-to-use state for delivering critical services and such systems shall be updated as and when new changes (for example OS patches, security patches, etc.) are implemented in the primary systems. This spare hardware shall regularly undergo testing in-line with the response and recovery plan of the REs. 6. REs shall take all necessary precautions while updating the 'golden' server images and data backup to ensure that server images and data backups are undamaged/unbroken. 7. In case of ransomware attacks that specifically target backups, conventional data backups may not be effective. Therefore, REs shall create backups in an isolated and immutable (and/ or air-gapped) manner to ensure recovery if production system is compromised. 8. REs shall undertake regular business continuity drills to check the readiness of the organization and effectiveness of existing security controls at the ground level. One such drill scenario recommended to be tested is recovering from a ransomware attack considering both PDC and DRS have been impacted. This shall assess the effectiveness of people, processes and technologies to deal with such attacks.	
RC.RP.S2	1. In the event of disruption of any one or more of the *critical systems*, the RE shall, within 30 minutes of the incident, declare that incident as 'Disaster' based on the business impact analysis. Accordingly, the RTO shall be two (2) hours as recommended by IOSCO[33] for the resumption of critical operations. The RPO shall be 15 minutes for all	All REs (Mandatory)

[33] Refer https://www.bis.org/cpmi/publ/d146.pdf.

Standards	CSCRF guidelines	Applicability
	REs. The recovery plan shall be scenario-based and in line with the RTO and RPO specified.	
	2. REs shall conduct comprehensive scenario-based cyber resilience testing at least 2 times in a financial year (periodicity of such testing shall be of 6 months), to validate their ability to recover and resume operations following a cybersecurity incident/ attack within prescribed RTO and RPO defined by SEBI. In this regard, REs shall incorporate extreme plausible cyber-attack scenarios into their cyber response and recovery planning. The said scenarios may be devised by REs in consultation with their respective *IT Committee for REs* based on the learning from various sources such as past cybersecurity incidents, near-miss analysis, data from Security Operations Centre, honeypot logs analysis, etc. 3. REs shall periodically conduct backup testing and restore back-up data to check its usability. 4. For cyber resilience testing, REs shall also include stakeholders such as critical third-party service providers, market intermediaries, linked REs, etc. 5. The result of the Cyber resilience testing shall be placed before *IT Committee for REs*. The lessons learned from conducting such cyber resilience testing shall be shared with SEBI within 3 months from the end of the relevant period of conducting cyber resilience testing. Status of the observations found during the cyber resilience testing shall be monitored and tracked by *IT Committee for REs*.	MIIs and Qualified REs (Mandatory)
RC.RP.S3	1. All REs shall conduct suitable periodic drills to test the adequacy and effectiveness of the response and recovery plan.	All REs (Mandatory)

Standards	CSCRF guidelines	Applicability
RC.RP.S4	1. A backup and recovery plan shall be formulated by the REs and approved by their respective *IT Committee for REs*. The backup and recovery plan shall include policies and software solutions that work together to maintain business continuity in the event of a security incident. Such plan shall include guidance on restoration of data with the backup software used by the RE. 2. The backup and recovery policy shall include backup of data as well as backup of server images. 3. The backup of data and server images shall be maintained at off-site locations to keep backup copies intact and unbroken. 4. RTO and RPO, as prescribed by SEBI from time to time, shall be included in the recovery plan for the restoration of systems after cybersecurity incidents.	All REs (Mandatory)
	5. REs shall maintain offline, encrypted backups of data and shall regularly test these backups at least on a quarterly basis to ensure confidentiality, integrity and availability of data.	MIIs and Qualified REs (Mandatory)
RC.CO: Guidelines		
RC.CO.S1, RC.CO.S2, RC.CO.S3	1. Recovery plans shall be discussed with *IT Committee for REs* by the REs. Such plans shall include stakeholders' coordination in recovery process, and both internal and external communication.	All REs
RC.IM: Guidelines		
RC.IM.S1	1. While ensuring protection of data, and security of processes, RE's BCP-DR capabilities shall support its cyber resilience objectives, and rapid recovery and resumption of critical operations after cybersecurity incident.	All REs

Standards	CSCRF guidelines	Applicability
	2. REs shall try to incorporate lessons learned from incidents reported (if any) by other REs.	
RC.IM.S2	1. RE's RTO shall be met for all interconnected systems and networks through capacity upgradations and periodic coordinated resilience testing. 2. Recovery plan shall be improved after analysing the learnings from periodic drills.	All REs (Mandatory)
Cyber Resilience goal: EVOLVE		
EV.ST: Guidelines		
EV.ST.S1, EV.ST.S2, EV.ST.S3	1. REs shall anticipate new attack vectors through threat modelling (based on risk assessment) and work to defend them. 2. REs shall strive for reducing their attack surfaces. 3. RE shall proactively examine controls, practices, and capabilities for prospective, emerging or potential threats. 4. RE shall proactively assess and take necessary actions with respect to its system's requirements, architecture, design, configuration, acquisition processes, or operational processes as a strategy for adaptation to the identified and prospective threats and vulnerabilities. 5. RE shall continuously improve upon the ability to quickly deploy and integrate existing and new services, both on-premises and in the cloud. 6. RE shall strive to rapidly correlate data using mathematical models and machine learning in order to make data-driven decisions. 7. REs shall use auditing/ logging systems on different OS to acquire and store audit/logging data.	All REs except small, self-certification REs

Standards	CSCRF guidelines	Applicability
	8. In order to include heterogeneity, apply different audit/logging regimes at different architectural layers. 9. REs shall look for feasibility of deploying diverse operating systems. Attack or compromise on one type of OS may not affect other OS deployed. 10. RE shall maintain extra capacity of IT assets for information storage, processing, or communications.	

Part III: Structured Formats for CSCRF Compliance

Annexure-A: VAPT Report Format

REPORTING FORMAT FOR MARKET ENTITIES TO SUBMIT THEIR COMPLIANCE AND FINDINGS OF VAPT

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD OF AUDIT: <>

NAME OF THE AUDITING ORGANISATION: <Name>

Date on which VAPT Report presented to 'IT Committee for REs': <Date>

RE's Authorised signatory declaration:

I/ We hereby confirm that the information provided herein is verified by me/ us and I/ we shall take the responsibility and ownership of this VAPT report.

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

1. Minutes of the Meeting (MoM) of 'IT Committee for REs' <Date> in which the VAPT report was approved.
2. VAPT report as submitted by the auditor

Table of Contents

This is to be submitted by the auditor on the RE's letter head.

1. **Auditor's Declaration**

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am a Partner/ Proprietor of firm <Name of the Auditing Organization> with CERT-In empanelment from <Date> to <Date>. I have conducted VAPT for <Name of the RE> period <….> as per the requirements of SEBI. The scope of VAPT covers following circulars/ guidelines/ advisories issued by SEBI:

Checklist for VAPT compliance as required:

S. No.	Area	Details (assets, applications, etc.) of the Audit area	Is the Entity Compliant? (Yes/ No)	Auditor's comments
1.	Vulnerability Assessment			
2	External Penetration Testing			
3.	Wi-Fi Testing			
4.	API Security Testing			
5.	VA and PT of mobile applications			
6.	Network segmentation testing			
7.	OS and DB Assessment			
8.	VAPT of cloud implementation			
9.	Configuration audit			

I confirm that the VAPT has been conducted as per the auditor's guidelines prescribed in this framework.

I also confirm that I have no conflict of interest in undertaking the above-mentioned VAPT activity.

For and on behalf of

Name:

Contact no.:

Place:

Date:

2. **Executive Summary**
   <Auditing Organization to provide an executive summary of the findings>

3. **Scope of VAPT**

Sr. No.	Type of Assessment	List the details of the assessment
1.	Vulnerability Assessment of Infrastructure – Internal and External	//List the count of IPs audited
2.	Vulnerability Assessment of Applications – Internal and External	//List the count of IPs audited
3.	External Penetration Testing – Infrastructure and Applications	//List the count of IPs audited
4.	Wi-Fi Testing	//List the number of Wi-Fi access points/ routers/ devices audited
5.	API Security Testing	//List the APIs audited
6.	Network Segmentation Testing	//List the network segmentation audited
7.	VA and PT of Mobile Applications	//List the number of APK files and IPA files audited
8.	OS and DB Assessment	// List the type and number of OS and DBs audited.
9.	VAPT of Cloud implementation and Deployments	//Name the cloud service provider and list the IPs audited
10.	Configuration audit	//List the systems for which configuration audit has been conducted

4. **Tools used**:
   4.1. *Name of the Tool*:
   4.2. *Type*: Open source/ Commercial
   4.3. *Operations*: manual/ automated/ both

5. **Exclusions, if any***:*

// Please enclose attachments regarding exclusions as approved by 'IT Committee for REs' along with MoM of the meeting where the exclusions were approved.

6. **Summary of the VAPT Report:**

6.3. Details of Vulnerability Assessment findings:

Sr. No.	**Vulnerability Assessment Findings Details**												
1.	Auditor (Name) for VA:												
2.	VA Start Date:												
3.	VA End Date:												
4.	Scope	Vulnerability Assessment											Auditor Remarks
5.		Number of Identified vulnerabilities					Closure Timelines	Open vulnerabilities (Shall be applicable during final submission)					
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total	
7.	Critical Assets												
8.	VA of infrastructure - Internal and External												
9.	VA of Applications - Internal and External												
10.	WiFi Testing												
11	API Security Testing												
12.	Network Segmentation												
13.	VA of mobile applications												
14.	OS and DB Assessment												
15.	VA of cloud deployments												

16	Configuration Audit												
17.	Others, please specify												

6.4. Details of Penetration Testing findings:

Sr. No.	**Penetration Testing Findings Details**												
1.	Auditor (Name) for PT:												
2.	PT Start Date:												
3.	PT End Date:												
4.	Scope	Penetration Testing											Auditor Remarks
5.		Identified vulnerabilities					Closure Timelines	Open vulnerabilities (Shall be applicable during final submission)					
6.		Critical	High	Medium	Low	Total		Critical	High	Medium	Low	Total	
7.	Critical Assets												
8.	External Penetration Testing - Infrastructure and Application												
9.	PT of mobile applications												
10.	PT of cloud deployments												
11.	Others, please specify												

7. **Detailed Report**

Detailed report to be submitted for all the items in the scope as per the below mentioned format (to be submitted only when sought by SEBI):

Sr. No	URL/ Application Name	Type of Risk (Critical/ High/ Medium/ Low)	Observations/ Vulnerability	Reference (CVE/ CWE/ OWASP/ Best Practice)	EPSS/ SSVC score	Impact	Recommendations	Management Comments with specific closure timelines
1.								
2.								
…								

8. Risk Rating description

Rating	Description
CRITICAL	The failure has an impact on the system delivery resulting in outage of services offered by the RE.
HIGH	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed within a reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls.

Annexure-B: Cyber Audit Report Format

Cyber audit report format for compliance submission

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD OF AUDIT: <>

NAME OF THE AUDITING ORGANISATION: <Name>

Date on Which Cyber Audit Report presented to 'IT Committee for REs' : <Date>

RE's Authorised signatory declaration:

I/ We hereby confirm that the information provided herein is verified by me/ us and I/ we shall take the responsibility and ownership of this cyber audit report.

Further, this is to certify that:

a. *Comprehensive measures and processes including suitable incentive/ disincentive structures, have been put in place for identification/ detection and closure of vulnerabilities in the organization's IT systems.*
b. *Adequate resources have been hired for staffing our Security Operations Centre (SOC).*
c. *There is compliance by us with CSCRF.*

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

1. Minutes of the Meeting (MoM) of 'IT Committee for REs' <Date> in which the cyber audit report was approved.
2. Cyber audit report as submitted by the auditor

Table of Contents

This is to be submitted by the auditor on the company's letter head.

1. **Auditor's Declaration**

TO WHOM SO EVER IT MAY CONCERN

This is to declare and certify that I am a Partner/Proprietor of firm <Name of the Auditing Organization> with CERT-In empanelment from <Date> to <Date>. I have conducted Cyber audit for <Name of the RE> period <….> as per the requirements of SEBI.

Checklist for Cyber audit as required:

S. No.	Area	Details of the audit area	Is the Entity Compliant? (Yes/No)	Auditor's comments
1.	Cybersecurity and Cyber resilience policy			
2.	Asset Inventory			
3.	Risk assessment and Risk management			
4.	Supply chain risk management			
5.	Awareness and Training			
6.	Data security			
7.	Security continuous monitoring			
8.	SOC efficacy			
9.	Incident Management and Response			
10.	Incident recovery planning			

I confirm that the audit has been conducted as per the auditor's guidelines prescribed in CSCRF (Cyber Audit).

I also confirm that I have no conflict of interest in undertaking the above-mentioned audit.

For and on behalf of

Name:

Contact no.:

Place:

Date:

2. Executive Summary
   <Auditing Organization to provide an executive summary of the findings>

3. Scope of audit/Terms of reference (as agreed between the auditee and auditor), including the standard/specific scope for audit:-

   3.1. List of SEBI Circulars/ Guidelines/ Advisories/ Letters covered:

S. No.	SEBI circular/ letter/ advisory	Issue date

   3.2. List of all IT infrastructure and geographical locations (including IT systems of PDC, DR, Near site, Co-lo facility) covered under audit

S. No.	List of IT infrastructure/ Geographical locations/ Third-party vendors	Details (assets ID, asset name, applications, etc.) of the Infrastructure assessed
1.	PDC	
2.	DR	
3.	Near-site	
4.	Co-location Facility (if applicable)	
5.	Cloud Infrastructure	
6.	Third-party service provider	
7.	Others	

   3.3. Any other specific item(s)

4. Methodology/ Audit approach (audit subject identification, pre-audit planning, data gathering methodology, sampling methodology etc. followed by the Auditing Organization)

5. Summary of findings (including identification tests, tools used and results of tests performed)

S.No	Number of Non-conformity	Number of observations	Risk rating				Any other comments
			Critical	High	Medium	Low	
1							

6. Control-wise Compliance status of SEBI CSCRF:

S.No	Standards prescribed by SEBI CSCRF (Clause number and text)	Description of Finding(s)/ Observation(s)	Name of the system belongs to RE or third-party vendor	Status/nature of findings	Risk rating (C/H/M/L) of the findings	C/I/A affected	Test cases used	Root Cause Analysis	Impact analysis	Auditor recommendations/ Corrective actions	Deadline of corrective action(s)	Management response	Whether similar issue was reported in the last three audits.	*List of documentary evidence including physical inspection/ sample size taken by the auditor
1	GV.OC.S1													
2	GV.OC.S2													
…														
N	EV.ST.S5													

*Explicit reference to the key auditee organisational documents (by date or version) including policy and procedure documents

7. A brief description of the above-mentioned compliance requirements is as follows-
   i. Standards prescribed by SEBI CSCRF (or any other cybersecurity circular/ letter/ guidelines) (Clause number and text)- The clause corresponding to this observation w.r.t CSCRF (or any other cybersecurity circular/ letter/ guidelines) issued by SEBI.
   ii. Description of findings/observations – Description of the findings in sufficient details, referencing any accompanying evidence
   iii. Name of system belongs to RE or vendor-(Self Explanatory term)

iv. Status/ Nature of Findings – The category can be specified, for example:
   a. Non-compliant (Major/Minor)
   b. Work in progress
   c. Observation

v. Risk Rating of the finding - A rating shall be given by the auditing organization for each of the observations, based on its impact and severity, to reflect the risk exposure as well as the suggested priority for action

Rating	Description
CRITICAL	The failure shall have impact on the system delivery resulting in outage of services offered by the RE.
HIGH	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to regulatory non-compliance, significant financial, operational and reputational loss. These observations need to be addressed with utmost priority.
MEDIUM	Represents weakness in control with respect to threat(s) that is/are sufficiently capable and impacts asset (s) leading to exposure in terms of financial, operational and reputational loss. These observations need to be addressed within a reasonable timeframe.
LOW	Represents weaknesses in control, which in combination with other weakness can develop into an exposure. Suggested improvements for situations not immediately/directly affecting controls. .

vi. C/I/A Affected **–** The principles of Confidentiality/ integrity/ availability affected due to issued left unaddressed**.**

vii. Test cases used **–**The details of test cases used for arriving at this observation. The test cases may also be provided as annexures with the report, if required.

viii. Root Cause analysis – A detailed analysis on the cause of the non-conformity.

ix. Impact Analysis **–** An analysis of the likely impact on the operations/ activity of the RE.

x. Auditor recommendations/ Corrective actions **–** The actions to be taken (by the RE) to correct the non-conformity.

xi. Deadline of corrective action(s) **-**The RE shall specify the deadline not only for the corrective action(s) to be taken on the system(s) where NC/ observation was found, but also specify the deadline for corrective action on systems with related functionalities/ configurations where similar observations could have been found/are found.

xii. Management response – Management action plan/taken to address the observation and/ or implementation of auditor's recommendation

xiii. Whether similar issue was reported in the last three audits – Yes/ No

xiv. List of documentary evidence including physical inspection/ sample size taken by the auditor

8. Format for exception reporting by the RE: These exceptions shall be approved by the *IT Committee for REs*

S. No.	Standard of CSCRF	Description of non-compliance	Auditor observation	Auditor recommendation	Management comments	Comment of 'IT Committee for REs'	Comments of Board of RE	Comments of Board of Trustee (wherever applicable)	Status of non-compliance (open/closed)	Repeat observation in last 3 audits	Deadline for corrective action	Risk category of non-compliance

9. The audit report shall also include the following-

9.1. Audit report shall provide terms of reference (ToR) of audit which shall indicate the scope/perimeter of the coverage of the systems audited in the cyber audit report regarding the compliances checked including areas (but not limited to) computer hardware, business applications, software, cyber governance, linkage with vendor systems/ other REs' systems like stock brokers, RTAs, Fund Accountants, email systems, etc.

9.2. Audit report shall include open observations from previous audits and comments of auditors for compliances checked for the same.

9.3. The auditor shall mention in the audit report the methodology adopted to check compliance. Further, the reason for disagreement between auditor and management, if any, shall also be recorded in audit report.

10. Any other relevant comments by the auditor:

11. Conclusion of cyber audit

Annexure-C: Recovery Plan Template (Reference Guide)

Recovery Plan Template for REs

1	Cybersecurity incident recovery plan	i. Preparation: Measures taken in preparation for cybersecurity incident (pre-incident).	
		ii. Identification Checklist	a. Source (Who has discovered or reported the incident?)
			b. When it was discovered?
			c. Details of the incident
			d. Incident occurred on on-prem/ cloud resource?
			e. What is the location (PDC/ DR/ Near DR, etc.) of the incident?
			f. The impact of the incident on the business operations
			g. What is the extent of the incident w.r.t applications and networks?
			h. Type of the incident (e.g. Phishing mail, weak credentials, ransomware attack, data breach, etc.)
			i. How did the Cybersecurity Incident occur?
		iii. Containment checklist	a. Can the incident be isolated to identify the scope of the incident and determine what systems, services, data or networks are compromised? If so, what are the steps taken, if not, explain why it can't be isolated?
			b. Are the affected systems kept isolated from the non-affected ones?
			c. Have the 'golden' server images and data been identified?
			d. Is the latest data backup (as per prescribed RPO) available?
			e. Have the copies of the infected machines preserved for digital forensics and incident response experts for analysis?
			f. Has the threat been removed from the infected devices?
		iv. Resolution checklist	Resolving the cause of the incident: a. Removing malware, b. Patching vulnerabilities, c. Taking other measures etc. Please specify resolution method.

		v. Recovery checklist	a. Recover lost or corrupted data, b. Restore normal operations by returning systems and networks to a known good state c. Taking other measures etc.
2	Cybersecurity incident recovery plan scenarios		
3	Categorization of incidents		
4	Key assumptions and pre-requisites		
5	Authorization		
6	Details of the Incident Response Team (IRT) (Internal/External)		
7	Details of other teams involved (Internal/External)		
8	Cybersecurity incident recovery invocation		
9	Off site location address where 'golden' copy of server images and data are stored		
10	Recover System(s) and Services		
11	Recovery Actions		
12	Lessons learned: Document lessons learned from the incident and incorporate them into incident response and recovery plans.		
13	Post-incident: Measures taken to avoid reoccurrence of the cyber incident		
14	Perform Hotwash		

Part IV: CSCRF Annexures and References

Annexure-D: Audit Guidelines

1. **Auditor Selection Norms for VAPT and Cyber Audit**
   a. Auditors must mandatorily be CERT-In empanelled.
   b. Auditor must preferably have a minimum 3 years of experience in IT audit of Banking and Financial services preferably in the Securities Market. E.g. Stock exchanges, clearing houses, depositories, stock brokers, depository participants, mutual funds, etc. The audit experience should have covered all the major areas mentioned under various cybersecurity frameworks and guidelines issued by SEBI from time to time. Auditing experience of the Cybersecurity Framework under ISO 27001 for an organization will be an added advantage.
   c. The Auditor must have experience in/ direct access to experienced resources in the areas covered under CSCRF. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security professional) from International Information systems Security Certification Consortium, commonly known as $(ISC)^2$.
   d. The Auditor shall have ISMS/ IT audit/ governance frameworks and processes conforming to leading industry practices like COBIT.
   e. The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the REs. It shall not have been engaged over the last two years in any consulting engagement with any departments/ units of the RE being audited.
   f. The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's Jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.
   g. The auditor must have experience of performing VAPT.
   h. The auditor must compulsorily use only licensed tools.
   i. The Auditor must compulsorily enter into a Non-disclosure Agreement (NDA) with the auditee. Under no circumstances, the data sought during the review or the audit report subsequently should leave the jurisdiction of India.

2. **Guidelines to Auditors**

   To conduct the cyber audit as per the provisions of CSCRF, following are the guidelines to be adhered to:

   a. RE shall ensure that NDA is signed between the RE and auditor prior to initiation of the cyber audit.

b. All audit reports shall be submitted strictly as per the format provided in CSCRF.
c. The coverage of the audit shall be as follows:
    i. REs which have been declared as CIIs by NCIIPC shall follow the guidelines/ circulars issued by NCIIPC for selecting sample size for critical/ non-critical assets.
    ii. Rest of the REs shall take the sample size as mentioned in 'CSCRF Compliance, Audit Report'.
    iii. RE shall ensure that 100% of their *critical systems* should get covered under cyber audit. Further, RE shall ensure that for 25% of non-critical systems, sample size and sampling method should be mentioned explicitly in the audit report with the rationale of checking it on sample basis and the chosen sample size.
    iv. As part of audit of the RE, the auditor shall verify, and certify, whether there is a clear delineation/ demarcation of roles and responsibilities between the RE and Hosted service provider (as given in definitions section). The auditor shall also verify, and certify, whether the above-mentioned demarcations of roles and responsibilities have been incorporated in the agreement/ contract signed between the RE and Hosted service provider.
d. The auditors shall also validate the adherence to the timelines as stated in '*Section 4: CSCRF Compliance, Audit Report Submission, and Timelines*' of CSCRF.
e. For mandatory guidelines, auditor shall verify whether guidelines have been implemented as mentioned in the CSCRF. If there are any variations, auditors shall mention the same with relevant evidences in their report.
f. For non-mandatory guidelines, auditors shall verify that whether REs have implemented equivalent controls or higher. If the implemented measures are not lower/ weaker than the stated guidelines, auditors shall mention the same with proper evidences in their report.
g. For standards where no guidelines are mentioned, auditors shall verify that REs have implemented the industry best practices.
h. Auditor shall ensure that the evidences are comprehensively stated with the observations made in the report. Auditors shall provide appropriate description of evidences verified for each standard/guidelines.
i. The risk-rating category (critical/ high/ medium/ low) shall be presented clearly in the audit observations.
j. Auditor shall compulsorily give their recommendations and suggestions to mitigate critical and high observations made in the report for the consideration of the REs. REs shall examine these recommendations and take it to their respective *IT committee for REs* for remediation.
k. REs shall securely store the evidences provided by the auditor. These evidences may be scrutinized during regulatory inspections/investigations.
l. Auditors shall verify the closure of previous audit observations and mention the status of the same in the audit report.

m. If any observation is repeated from the previous audit, auditor shall clearly mention them as repeat observation.
n. Auditor's report(s) shall include assessment of identification of assets as critical/ non-critical.
o. Auditor's report(s) shall be accompanied by the auditor's certificate for adhering to the above-mentioned points.

3. **Other recommended references:**
   a. IT Security Auditing Guidelines for REs: https://www.cert-in.org.in/PDF/guideline_auditee.pdf
   b. Guidelines for CERT-In empanelled Information Security Auditing Organizations: https://www.cert-in.org.in/PDF/Auditor_Guidelines.pdf

Annexure-E: Scenario-based Cyber Resilience Testing

Scenario-based Cyber Resilience Testing

This is a sample template for Stock Exchange. REs are encouraged to make their scenarios in consultation with their *IT Committee for REs*. Sample scenarios that are targeted to cover in Cyber Response plan as well as Cyber Resiliency Testing (Types of Attack × Potential Targeted Time intervals- On Core Systems):

	Cyber Attack-> Time Interval	**DDoS**	**Malware/ Malicious Code Attack**	**Application Level Attacks (SaaS Model)**	**DNS Based Attacks (Internal & Internet)**	**Brute Force/Authentication based attack**	**AD attack**
Pre-open Sessions	Before BOD/early Morning						
	Before 9:00 hrs						
	B/W 9:00 - 9:15 hrs						
Regular Trading Sessions	09:15 - 15:30 hrs						
Closing Session	15:30 -16:00 hrs						
	Post 16:00 hrs						

Attack Scenario Category	Types of attacks	Impact	Response & Recovery
DDOS		Service Unavailability	DDOS Protection services for auto mitigation.
Malware Attacks	Ransomware	Service Unavailability, Data Corruption, Data exfiltration, Website Defacement	1. Isolate and contain the infected systems from overall network. Block IOCs, DNS traffic.
	Spyware		2. Restrict administrative and system access.
	Trojans		3. Monitor network traffic.
	Worms		4. Restore OS, application and data from existing backups.
	Bots		
Application Level Attacks	Injection	Service Unavailability, Website Defacement	1. Monitor network traffic and logs.
	Broken Authentication & Session Management		2. Disable suspected user accounts and change access credentials.
	Cross-Site Scripting/request forgery		3. Apply patches/changes for vulnerability.

Attack Scenario Category	Types of attacks	Impact	Response & Recovery
DNS Based Attacks	DNS Spoofing/Cache Poisoning	Service Unavailability	1. Analyse the traffic requests.
	DNS Flood Attack		2. Restore DNS entries
	DNS Encoding		3. Monitor the DNS requests and responses
Social Engineering Attacks	Phishing, QRishing	It is a method, It may lead to any of the other attack	Spam filtering policy should be configured in available tools as a precaution.
Watering hole	Targeted individuals, organization, group of people	Website infection, Service Unavailability	1. Coordination with respective agency/website owner.
			2. Isolation of affected systems.
			3. Clean/replace the affected system.
Brute Force	Trial and Error approach	Service Unavailability, Unauthorized Access	1 Proper account locking mechanism.
	Authentication Based Attack		2 Monitoring
Active Directory Attack	Inappropriate access.	Data Confidentiality, compromised user accounts, new user creation	1.Review default security settings.
			2.Least privilege in AD roles.

Annexure-F: Guidelines on Outsourcing of Activities

SEBI's existing circulars on outsourcing by REs are as follows:

- *'Outsourcing of activities, Business Continuity Plan (BCP) and Disaster Recovery (DR) and Cyber Security and Cyber Resilience framework - Limited Purpose Clearing Corporation (LPCC)*' dated Nov 06, 2020
  (Refer: https://www.sebi.gov.in/legal/circulars/nov-2020/outsourcing-of-activities-business-continuity-plan-and-disaster-recovery-and-cyber-security-and-cyber-resilience-framework-limited-purpose-clearing-corporation_48106.html)

- '*Outsourcing of activities by Stock Exchanges and Clearing Corporations*' dated Sep 13, 2017
  (Refer: https://www.sebi.gov.in/legal/circulars/sep-2017/outsourcing-of-activities-by-stock-exchanges-and-clearing-corporations_35932.html)

- '*Outsourcing by Depositories*' dated Dec 09, 2015
  (Refer: https://www.sebi.gov.in/legal/circulars/dec-2015/outsourcing-by-depositories_31219.html)

- '*Guidelines on Outsourcing of Activities by Intermediaries*' dated Dec 15, 2011
  (Refer: https://www.sebi.gov.in/legal/circulars/dec-2011/guidelines-on-outsourcing-of-activities-by-intermediaries_21752.html)

Annexure-G: Application Authentication Security

Illustrative Measures for Application Authentication Security are given below:

1. Any Application offered by REs to Customers containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as “Application” hereafter) over the Internet should be password protected. A reasonable minimum length (and no arbitrary maximum length cap or character class requirements) should be enforced. While it is difficult to quantify password “complexity”, longer passphrases have more entropy and offer better security in general. REs should attempt to educate Customers of these best practices.
2. Passwords, security PINs etc. should never be stored in plain text and should be one-way hashed using strong cryptographic hash functions (e.g.: bcrypt, PBKDF2) before being committed to storage. It is important to use one-way cryptographic hashes to ensure that stored password hashes are never transformed into the original plaintext values under any circumstances.
3. For added security, a multi-factor (e.g.: two-factor) authentication scheme may be used (hardware or software cryptographic tokens, VPNs, biometric devices, PKI etc.). In case of IBTs and SWSTs, a minimum of two-factors in the authentication flow are mandatory.
4. In case of Applications installed on mobile devices (such as smartphones and tablets), a cryptographically secure biometric two-factor authentication mechanism may be used.
5. After a reasonable number of failed login attempts into Applications, the Customer’s account can be set to a “locked” state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer’s registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the Customer’s registered mobile number, or manually by the Broker after verification of the Customer’s identity etc.
6. Avoid forcing Customers to change passwords at frequent intervals which may result in successive, similar, and enumerated passwords. Instead, focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases. Customers may be reminded within reasonable intervals to update their password and multi-factor credentials, and to ensure that their out-of-band authentication reset information (such as e-mail and phone number) are up-to-date.
7. Both successful and failed login attempts against a Customer’s account may be logged for a reasonable period of time. It is recommended that measures such as CAPTCHAs or rate-limiting be used in Applications to thwart manual and automated brute force and enumeration attacks against logins.

Annexure-H: Data Security on Customer Facing Applications

Illustrative Measures for Data Security on Customer Facing Applications are given below:

1. Analyse the different kinds of sensitive data shown to the Customer on the frontend application to ensure that only what is deemed absolutely necessary is transmitted and displayed.
2. Wherever possible, mask portions of sensitive data. For instance, rather than displaying the full phone number or a bank account number, display only a portion of it, enough for the Customer to identify, but useless to an unscrupulous party who may obtain covertly obtain it from the Customer's screen. For instance, if a bank account number is "123 456 789", consider displaying something akin to "XXX XXX 789" instead of the whole number. This also has the added benefit of not having to transmit the full piece of data over various networks.
3. Analyse data and databases holistically and draw out meaningful and "silos" (physical or virtual) into which different kinds of data can be isolated and cordoned off. For instance, a database with personal financial information need not be a part of the system or network that houses the public facing websites of the REs. They should ideally be in discrete silos or DMZs.
4. Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is infeasible for certain personnel such as System Administrators and developers to not have privileged access to production databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.
5. Use industry standard, strong encryption algorithms (eg: RSA, AES etc.) wherever encryption is implemented. It is important to identify data that warrants encryption as encrypting all data is infeasible and may open up additional attack vectors. In addition, it is critical to identify the right personnel to be in charge of, and the right methodologies for storing the encryption keys, as any compromise to either will render the encryption useless.
6. Full-disk Encryption (FDE) for protecting sensitive data-at-rest at the hardware level by encrypting all data on a disk drive shall be used wherever possible. File-based Encryption (FBE) encrypts specific files or directories instead of the complete data on a disk. Therefore, both FDE and FBE with strong industry-standard algorithms shall be used together.
7. Ensure that all critical and sensitive data is adequately backed up, and that the backup locations are adequately secured. For instance, on servers on isolated networks that have no public access endpoints, or on-premise servers or disk drives that are off-limits to unauthorized personnel. Without up-to-date backups, a meaningful recovery from a disaster or cyber-attack scenario becomes increasingly difficult.

Annexure-I: Data Transport Security

Illustrative Measures for Data Transport Security are given below:

1. When an Application transmitting sensitive data communicates over the Internet with MIIs'/RE's systems, it should be over a secure, encrypted channel to prevent Man-In-The-Middle (MITM) attacks, for instance, an IBT or a Back office communicating from a Customer's web browser or Desktop with the RE's systems over the internet, or intra or inter organizational communications. Strong transport encryption mechanism such as TLS (Transport Layer Security, also referred to as SSL) should be used.
2. For Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server is mandatory, making the transport channel HTTP(S).
3. Avoid the use of insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, etc.

Annexure-J: Framework for Adoption of Cloud Services

SEBI's '*Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)*' circular dated March 06, 2023:

(Refer: https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html)

Annexure-K: Cyber Capability Index (CCI)

REPORTING FORMAT FOR MIIs AND QUALIFIED REs TO SUBMIT THEIR CCI SCORE

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD: <>

NAME OF THE AUDITING ORGANISATION (applicable for MIIs): <Name>

RE's Authorised signatory declaration:

I/ We hereby confirm that Cyber Capability Index (CCI) has been verified by me/ us and I/ We shall take the responsibility and ownership of the CCI report.

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

1. CCI report as per the format given in Table 27 and CCI score

Cyber Capability Index (CCI)

A. **Background**-

CCI is an index-framework to rate the preparedness and resilience of the cybersecurity framework of the Market Infrastructure Institutions (MIIs) and Qualified REs. While MIIs are required to conduct third-party assessment of their cyber resilience on a half-yearly basis, Qualified REs are directed to conduct self-assessment of their cyber resilience on an annual basis.

B. **Index Calculation Methodology**-

1. The index is calculated on the basis of 23 parameters. These parameters have been given different weightages.
2. Implementation evidence to be submitted to SEBI only on demand.
3. All implementation evidences shall be verified by the auditor for conducting third-party assessment of MIIs.
4. The list of CCI parameters, their corresponding target and weightages in the index, is as follows:

Table 27: CCI parameters with corresponding measure, implementation evidence, target, and weightage

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
1.	Security Budget Measure **[GV.RR.S4]**	Information Security Goal: Provide resources necessary for information systems.	Percentage (%) of the organisation's information system budget devoted to information security.	Impact	(Information security budget/ total organisation's information technology budget) ×100	10%	1. What is the total information security budget across all organization's systems? 2. What is the total information technology budget across all organization's systems? 3. Approval Document from Competent Authority for the same.	8%		
2.	Vulnerability Measure **[DE.CM.S5]**	Objective of this measure is to ensure that the vulnerabilities in organization's systems are identified and mitigated	Percentage of vulnerabilities mitigated pertaining to organization in a specified time frame.	Effectiveness Measure	(Number of vulnerabilities mitigated/ Number of vulnerabilities identified)×100	100 %	1. Confirmation that VAPT is done by CERT-In empanelled IS auditing organization and as per the scope prescribed by SEBI	18%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							2. VAPT report and its closure report. 3. Time taken to close the identified vulnerabilities.			
3.	Security Training Measure **[PR.AT.S1]**	Information Security Goal: Ensure that organization's personnel are adequately trained to carry out their assigned information security- related duties and responsibilities	Percentage (%) of information system security personnel that have received security training within the past one years.	Implementation	(Number of information system security personnel that have completed security training within the past year/total number of information system security personnel) ×100	100 %	1. Details of the training/ awareness sessions scheduled within the past 1 year. 2. Cyber audit observation against Standard 1 mentioned in 'Protect: Awareness and Training' header in CSCRF Part-I and respective guidelines in Part-II.	5%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
4.	Remote Access Control Measure **[PR.AA.S12]**	Information Security Goal: Restrict access to information, systems, and components to individuals or machines that have been authenticated and are identifiable, known and credible.	Percentage (%) of remote users logging through MFA.	Effectiveness	(Number of remote users logging through MFA/ total number of remote users) ×100	100 %	1. Does the organization use automated tools to maintain an up-to-date record that identifies all remote access points? 2. How many remote access points exist in the organization's network? 3. Does the organisation employ IDS or IPS to monitor traffic traversing remote access points? 4. Does the organisation collect and review audit logs associated with all remote	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							access points? 5. Evidence of users who are allowed remote access through MFA, validated through Firewall, AD, or any dedicated system. 6. Based on reviews of the incident database, IDS/ IPS logs and alerts, and/ or appropriate remote access point log files, how many access points have been used to gain unauthorized access within the reporting period?			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
5.	Audit Record Review Measure **[DE.CM.S1]**	Information Security Goal: Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, suspicious or abnormal activity.	Percentage (%) of *critical systems* integrated with SIEM.	Efficiency	(Number of *critical systems* integrated with SIEM tool/total number of *critical systems*) ×100	100 %	1. Is logging activated on the system? 2. Does the organization have clearly defined criteria for what constitutes evidence of "suspicious or abnormal" activity within system audit logs? 3. For the reporting period, how many system audit logs have been reviewed for past six months for suspicious or abnormal activity.	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
6.	Configuration Changes Measure **[DE.CM.S5]**	Information Security Goal: Establish and maintain baseline configuration and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Percentage (%) approved and implemented configuration changes identified in the latest automated baseline configuration.	Implementation	(Number of approved and implemented configuration changes identified in the latest automated baseline configuration/ total number of configuration changes identified through automated or manual scans) × 100	100 %	1. Does the organization manage configuration changes to information systems using an organizationally approved process? 2. Does the organization use automated scanning to identify configuration changes that were implemented on its systems and networks? 3. If yes, how many configuration changes were identified through	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							automated scanning over the last reporting period? 4. How many change control requests were approved and implemented over the last reporting period? 5. Cyber audit observation against Standard 3 mentioned in 'Detect: Continuous Security Monitoring' header in CSCRF Part-I and respective guidelines in Part-II.			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
7.	Contingency Plan Testing Measure **[RS.MA.S3]**	Information Security Goal: Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery of organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.	Percentage (%) of information systems that have conducted contingency plan testing at least once in a year.	Effectiveness	(Number of information systems that have conducted contingency plans testing at least once in a year/ number of information systems in the system inventory) ×100	100 %	1. How many information systems are in the system inventory? 2. How many information systems have an approved contingency plan? 3. How many contingency plans were successfully tested within the past 1 year? 4. Reports of the contingency plan testing conducted in past one year.	4%		

8.	User Accounts Measure **[PR.AA.S 7]**	Information Security Goal: All privilege users are identified and authenticated in accordance with information security policy.	Percentage (%) of privileged access through PIM.	Effectiveness	(Number of systems accessed through PIM/ total number of systems) ×100	100 %	1. Organization should have a documented and approved access control policy for systems, applications, networks, databases etc. 2. How many users have access to the system? 3. How many users have access to shared accounts? 4. Cyber audit observation against Standard 7 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in CSCRF Part-I and respective guidelines in Part-II.	3%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
9.	Incident Response Measure **[RS.CO.S 2]**	Information Security Goal: Track, document, and report incidents to appropriate organizational officials and/or authorities.	Percentage (%) of incidents reported within required time frame.	Effectiveness	(number of incidents reported on time/ total number of reported incidents) ×100	100 %	1. How many incidents were reported during the period? 2. Of the incidents reported, how many were reported within the prescribed time frame?	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
10.	Maintenance Measure **[PR.MA.S1]**	Information Security Goal: Perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Percentage (%) of system components that undergo maintenance in accordance with planned maintenance schedules.	Efficiency	(Number of system components that undergo maintenance according to planned maintenance schedules/ total number of system components) ×100	100 %	1. Does the system have a planned maintenance schedule? 2. How many components are contained within the system? 3. How many components underwent maintenance in accordance with the planned maintenance schedule?	5%		
11.	Media Sanitization Measure **[PR.AA.S14]**	Information Security Goal: Sanitize or destroy information system media before disposal	Percentage (%) of media that passes sanitization procedures testing.	Effectiveness	(Number of media that passes sanitization procedures testing/total number of media disposed or	100 %	1.Policy/procedure for sanitizing media before it is discarded or reused. 2. Indicative proof that policy is being	2%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
		or release for reuse.			released for reuse) × 100		followed. 3. Cyber audit observation against Standard 14 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in CSCRF Part-I and respective guidelines in Part-II.			
12.	Physical Security Incidents Measure **[PR.AA.S10** **]**	Information Security Goal: Integrate physical and information security protection mechanisms to ensure appropriate protection of the organization's	Percentage (%) of physical security incidents allowing unauthorized entry into facilities containing information systems.	Effectiveness	(Number of physical security incidents allowing unauthorized entry into facilities containing information systems/total number of physical security incidents) ×100	0%	1.Policy/procedure ensuring the secure physical access to *critical systems*? 2. How many physical security incidents occurred during the specified period? 3. How many of the physical	1%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
		information resources.					security incidents allowed unauthorized entry into facilities containing information systems? 4. Cyber audit Observation against Standard 10 mentioned in 'Protect: Identity Management, Authentication, and Access Control' header in CSCRF Part-I and respective guidelines in Part-II.			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
13.	Planning Measure **[GV.RR.S5]**	Information Security Goal: Develop, document, periodically update, and implement security measures for authorised access to the information systems of the organisation.	Percentage of employees who get authorized access to information systems only after they sign an acknowledgement that they have read and understood confidentiality and integrity agreement.	Implementation	(Number of users who are granted system access after signing confidentiality and integrity agreement/total number of users who are granted system access) ×100	100 %	1. How many users accessed the system? 2. How many users signed confidentiality and integrity agreement acknowledgements? 3. How many users have been granted access to the information system only after signing confidentiality and integrity agreement acknowledgements?	1%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
14.	Personnel Security Screening Measure **[PR.AA.S10]**	Information Security Goal: Ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions.	Percentage (%) of individuals screened before being granted access to organizational information and information systems.	Implementation	(Number of individuals screened/total number of individuals having access to organization's information and information systems) ×100	100 %	1. How many individuals have been granted access to organizational information and information systems? 2. What is the number of individuals who have completed personnel screening?	1%		
15.	Risk Assessment Measure **[ID.RA.S2]**	Objective of this measure is to periodically assess the risk to organization's IT assets and operations. Cybersecurity risks to the organization's	Percentage of organization's information systems, and assets covered under risk assessment.	Implementation Measure	(Number of organization's information systems, and assets covered under risk assessment/Total number of organization information	100 %	1. Has the organization completed a cyber-risk assessment? 3. Cyber Audit observation against this Standard 2 mentioned in 'Identify: Risk	5%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
		information systems, and assets are understood and assessed.			systems, and assets) ×100		Assessment' header in CSCRF Part-I and respective guidelines in Part-II.			
16.	Service Acquisition Contract Measure **[GV.SC.S3]**	Information Security Goal: Ensure third-party providers employ adequate security measures to protect information, applications, and/or services outsourced by the organization.	Percentage (%) of system and service acquisition contracts that include security requirements and/or specifications.	Implementation	(Number of system and service acquisition contracts that include security requirements and specifications/ total number of system and service acquisition contracts) ×100	100 %	1. How many active service acquisition contracts does the organization have? 2. How many active service acquisition contracts include security requirements and specifications? 3. How many contracts includes integration of systems with SOC technologies?	3%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							4. Whether the acquisition contract includes SLA for vulnerabilities closure and timely implementation of patches? 5. Contracts for adoption of Cloud includes implementation of 'security of the cloud' , etc.			
17.	System and Communication Protection Measure **[PR.DS.S4]**	Information Security Goal: Allocate sufficient resources to adequately protect electronic information infrastructure.	Percentage of mobile computers and devices that perform all cryptographic operations.	Implementation	(Number of mobile computers and devices that perform all cryptographic operations/total number of mobile computers and devices) ×100	100 %	1. How many mobile computers and devices are used in the organization? 2. How many mobile computers and devices employ cryptography? 3. How many mobile	1%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
							computers and devices have cryptography implementation waivers?			

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
18.	Risk Management **[GV.RM.S1, GV.RM.S2]**	Based on risk appetite of the organization, cybersecurity risks are identified, analysed, evaluated, prioritized, responded, and monitored.	Percentage (%) of organization information systems, and assets covered under risk management.	Effectiveness	(Number of organization information systems, and assets covered under risk management/Total number of organization information systems, and assets) ×100	100 %	1. Does organization have a cyber-risk management framework? 2. Has the organization established, communicated, and maintained its risk appetite and risk tolerance statements? 3. Has organization responded to risk observations based on its risk appetite?	8%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
19.	Critical Assets Identified **[ID.AM.S1, ID.AM.S2]**	Objective of this measure is to ensure identification and management of assets in accordance with their relative importance to the organizational objectives and the organization's risk strategy.	Percentage (%) of the *critical systems* identified by REs among all other IT systems.	Implementation Measure	(Number of critical systems Identified/ Total IT systems integrated with SOC) ×100	50%	1. Process to identify and approve the list of critical assets. 2. List of critical assets identified as per the ID.AM.S1. 3. Auditors reports on identification of assets as critical/ non-critical.	9%		
20.	CSK Events **[RS.MA.S5]**	Objective of this measure is to mitigate threats upon external IPs	Number of CSK reported events closed in timely manner.	Effectiveness Measure	(Total number of CSK reported events closed in 15 days/ Total number of CSK reported events to the organization)×100	100 %	1. Summary report of the events reported by CSK.	4%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
21.	Cybersecurity Policy Document **[GV.PO.S1]**	Develop, document, periodically update, and implement cybersecurity policies and procedures for organizational information systems that describe the security controls in place or planned for information systems.			Non quantifiable measure		1. Cybersecurity Policy document of the organization. 2. Frequency of the revision of the policy document. 3. Approval of the policy document. 4. Cyber audit observation against Standard 1 mentioned in 'Governance: Policy' header in CSCRF Part-I and respective guidelines in Part-II.	4%		

S No	Measure ID	Goal/Objective	Measure	Measure Type	Formula	Target	Implementation Evidence	Weightage	Self-assessment score	Auditor comments w.r.t. cyber audit (for MIIs)
22.	SOC efficacy	How effective is our SOC operational?	SOC efficacy score	Effectiveness	As specified in SOC efficacy (**Annexure-N**)	100 %	1. How effective is the functioning of RE's SOC?	5%		
23.	Automated compliance with CSCRF	Develop an automated tool (preferably integrated with log aggregator) to submit compliance with CSCRF.	Percentage (%) of standards compliance automated	Maturity measure	(Number of standards for which compliance has been automated for CSCRF compliance/Total number of CSCRF standards)×100	100 %	1. Automated dashboard to get detailed reports of CSCRF standards compliance.	5%		

5. Based on the value of the index, the cybersecurity maturity level of the MIIs and Qualified REs shall be determined as follows:

SN.	Rating	Index Score Rating
1	Exceptional Cybersecurity Maturity	100-91
2	Optimal Cybersecurity Maturity	90-81
3	Manageable Cybersecurity Maturity	80-71
4	Developing Cybersecurity Maturity	70-61
5	Bare Minimum Cybersecurity Maturity	60-51
6	Fail	< =50 (The RE has scored below the cut-off in at least one domain/ sub-domain)

6. MIIs and Qualified REs shall strive for building an automated tool and suitable dashboards (preferably integrated with log aggregator) for submitting compliance. A dashboard shall be available at the time of cyber audit, onsite inspection/ audit by SEBI or any agency appointed by SEBI.

Annexure-L: VAPT Scope

Comprehensive Scope for Vulnerability Assessment and Penetration Testing (VAPT)

1. The scope of the IT environment taken for VAPT should be made transparent to SEBI and should include all critical assets and infrastructure components including (not limited to) Networking systems, Security devices, Servers, Databases, Applications, Systems accessible through WAN, LAN as well as with public IP's, websites, etc.

   The scope should include (not limited to):

S. No.	VAPT scope
1.	VA of Infrastructure-Internal & External
2.	VA of Applications-Internal & External
3.	External Penetration Testing-Infrastructure & Application
4.	WIFI Testing
5.	API Security Testing
6.	Network Segmentation
7.	VA & PT of Mobile applications
8.	OS & DB Assessment
9.	VAPT of Cloud implementation and deployments
10.	Configuration audit

2. **Testing methodology:** The VAPT should provide in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks. The testing methodology should adapt from the following:
   a. SEBI CSCRF
   b. National Critical Information Infrastructure Protection Centre (NCIIPC)
   c. CERT-In Guidelines
   d. The National Institute of Standards and Technology ("NIST") Special Publication 800-115
   e. Latest ISO27001
   f. PCI-DSS standards
   g. Open Source Security Testing Methodology Manual ("OSSTMM")
   h. OWASP Testing Guide

Annexure-M: Cyber-SOC Framework for MIIs

SEBI's 'Cyber-SOC Framework for MIIs' circular ('*Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporations and Depositories*' dated Dec 07, 2018):

(Refer: https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html)

Annexure-N: Functional Efficacy of SOC

REPORTING FORMAT FOR FUNCTIONAL EFFICACY OF SOC

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD: <>

RE's Authorised signatory declaration:

I/ We hereby confirm that report of functional efficacy of SOC has been verified by me/ us and I/ We shall take the responsibility and ownership of the report.

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

1. Report of functional efficacy of SOC as per the format given in Table 28 to Table 34.

Measuring and auditing functional efficacy of SOC

1. SEBI has formulated a quantifiable method with five broad domains to gauge the functional efficacy of SOC.
2. REs are required to calculate the scores in all the five areas to arrive at the final score of SOC efficacy. The calculation[34] of the final score is described below:

Table 28: Score calculation of SOC efficacy

Sr. No.	Domain	Weightage (%) [A]	Score [B]	Normalised Score [S] = (B×A)/100
1	Coverage of assets w.r.t SOC technologies	25		**C**
2	SOC Operations	25		**Y**
3	Competency of deployed SOC Personnel	20		**P**
4	SOC Governance	15		**H**
5	SOC Enrichments and Enhancements	15		**E**
FINAL SCORE (ΣS)				

3. The detailed scoring system for the above mentioned domains is given below:
   a) Coverage of assets w.r.t SOC technologies: Integration of all assets with deployed SOC technologies is required in order to have holistic visibility over RE's IT environment. It shall help the RE in measuring the extent to which SOC technologies encompass the RE's entire asset base.

Table 29: IT Asset distribution of RE

Sr. No.	System Types*	System Type ID	Count
1	Network Devices (Switches, Load Balancers, Routers, Firewalls, etc.)	S1	
2	Security Solutions (SOC and NOC technologies deployed)	S2	
3	End-Points	S3	
4	Applications (Internal or External)	S4	
5	Databases	S5	
6	All Servers (such as AD, DHCP, DNS, Patch mgmt., NTP, IPT, WiFi, Application server, Database servers , server-based security solutions, etc.)	S6	
n		Sn	

**The data in Table 29 shall be extracted from Asset Inventory. If there is some other category of systems in the asset inventory maintained by REs, the same may be added in this table with another category and based on applicability, it may be added to Table 30.*

Table 30: Methodology to assess the level of asset integration with SOC Technologies

[34] For the purpose of calculation, zero score shall be given for a category/ sub-category if the denominator is zero.

Sr. No.	SOC Technologies	Weightage (%) (W)	Systems ID applicable	Count of Systems to be integrated (x) *[to be identified from table 29]*	Count of Systems Actually Integrated and covered (y)	Coverage Score Z=(y/x)	Weighted Score (Z×W)
1	PAM	10	S1, S2, S4, S5, S6				
2	Anti-virus/ EPP	10	S3, S6				
3	EDR	10	S3, S6				
4	DLP	10					
5	DAM	10	S5				
6	WAF	10	S4				
7	Email-gateway*	10					
8	Web-gateway/ Proxy*	10					
9	DDoS*	10					
10	SIEM	10	S1, S2, S4, S5, S6				
n							
Technology-Asset-Coverage-percentage							**C**

b) <u>SOC Operations:</u> To determine the efficiency of the periodic activities carried out by SOC personnel for effective threat management and regular maintenance of SOC technologies.

<u>Table 31: Methodology to assess the performance of SOC operations</u>

Sr. No.	Metric	Value	Weightage (W) (%)	Weighted Score
1	**Log ingestion into SIEM**		5	(A/B)×W
	Log sources reporting to SIEM [A]	A		
	Total No. of Log Sources (from Table 29) [B]	B		
2	**Latency in Log Ingestion (benchmarking against 5 minutes)**		5	IF C<5 then score = ((5-C)/5)×W IF C>=5 then score = 0
	Maximum log processing latency- latency between collection of the security event at the log source and processing it in SIEM (in minutes) [C]	C		

Sr. No.	Metric	Value	Weightage (W) (%)	Weighted Score
3	**SOC technology version control**		5	(D/E)×W
	No. of technologies running on version 'n-1' and 'n' [D]	D		
	Total No. of technologies deployed [E]	E		
4	**SOC technology vulnerability closure**		5	(F/G)×W
	No. of open advisories (issued by CERT-In/ CSIRT-Fin) and vulnerabilities on SOC technologies [F]	F		
	Total advisories (issued by CERT-In/ CSIRT-Fin) and vulnerabilities reported on SOC technologies [G]	G		
5	**SIEM Use cases**		5	(H/I)×W
	No. of SOC technologies for which use cases are configured [H]	H		
	Total no. of SOC technologies [I] (from Table 30)	I		
6	**Use cases that are not triggered**			
	Use-cases that are not triggered [J]	J	5	((K-J)/K)×W
	Total no. of use cases [K]	K		
7	**Playbooks Defined**		10	(L/M)×W
	No. of playbooks defined associated with use cases [L]	L		
	Total no. of use cases [M]	M		
8	**False Positives**		10	((O-N)/O)×W
	No. of false positives [N]	N		
	Total no. of alerts [O]	O		
9	**False Negatives**		10	((Q-P)/Q)×W
	No. of false negatives [P]	P		
	Total no. of alerts [Q]	Q		
10	**Threat Intel (benchmarking against 60 minutes)**		5	IF R<60 then score = ((60-R)/60)×W IF R>=60 then score = 0
	Mean Time to process the Threat Intel feed received (minutes) (R)	R		
11	**Handling Critical Systems**			
	Critical Applications and assets' log ingestion in SIEM is being verified on a daily basis?	Yes=1, No=0 (S)	2	S×W
	Critical Applications and assets' integration with Anti-virus/ EDR, DAM, etc. verified on a daily basis?	Yes=1, No=0 (T)	2	T×W

Sr. No.	Metric	Value	Weightage (W) (%)	Weighted Score
	Use-cases/rules configured on SIEM for *critical systems*?	Yes=1, No=0 (U)	2	U×W
	Privilege access to *critical systems* verified on a weekly basis?	Yes=1, No=0 (V)	2	V×W
	Configuration and data back-ups being taken periodically?	Yes=1, No=0 (X)	2	X×W
	Total		**75**	**Y**

**The above metric for SOC operations is not exhaustive, REs are required to add other metrics depending upon the maturity of their security infrastructure and availability of tools and technologies. 25% weightage is left to the REs.*

c) <u>Competency of deployed SOC personnel:</u> To assess the skill level of security professionals deployed in SOC through a combination of appropriate industry level certifications and years of experience to ensure that SOC operations are carried out in smooth and effective manner.

<u>Table 32: Methodology to assess the competency of deployed SOC personnel</u>

Sr. No.	Category of engineers	Minimum Certification requirement	Weightage of category [C] (%)	Years of Experience (YoE)	Weightage of sub-category [w]	Count of Engineers having minimum required certifications# [x]	Actual sub-category Score [z] = [x] × [w]	category-wise score [A] = Sum [z] / Sum[x]	Weighted Score [B] = [A] × [C]
1	L1	CEH	35	2	0.25				
2				3	0.50				
3				4	0.75				
4				5	1.00				
5	L2	CEH + Any product OEM certification	25	6	0.33				
6				7	0.66				
7				8	1.00				
8	L3	CEH + CISM	40	9	0.25				
9				10	0.50				

Sr. No.	Category of engineers	Minimum Certification requirement	Weightage of category [C] (%)	Years of Experience (YoE)	Weightage of sub-category [w]	Count of Engineers having minimum required certifications# [x]	Actual sub-category Score [z] = [x] × [w]	category-wise score [A] = Sum [z] / Sum[x]	Weighted Score [B] = [A] × [C]
10				11	0.75				
11				>=12	1.00				
Final Score of Manpower									**P**

#Fractional YoE shall be converted to be the floor value of the experience for calculation. Example: if an engineer has 2.6 YoE then it has to be counted in the category of 2 YoE. Engineers not having required minimum certification cannot be counted in the category.

d) <u>SOC Governance:</u> To determine the capability of strategic management and the level of oversight of SOC through factors such as finances, personnel training and the involvement of IT Committees for REs and their Board.

<u>Table 33: Methodology to assess the governance of SOC</u>

Sr. No.	Metric	Value (A)	Weightage (W)(%)	Weighted Score
1	**Budget for SOC**		45	(2*B/A)×W *(maximum score can be 45)*
	Budget spent on cybersecurity [A]	A		
	Budget Spent on SOC technology and governance (50% benchmarking) [B]	B		
2	**Training**			
	Percentage of budget spent for training out of total budget forecasted for training	E	10	(E/100)×W
3	Whether SOC review has been undertaken by *IT Committee for REs*	Yes=1, No=0 (F)	5	F×W
4	Whether recommendations of technology committee have been submitted to governing board of RE	Yes=1, No=0 (G)	5	G×W
Total			**65**	**H**

**The above metric for SOC operations is not exhaustive, REs are required to add other metrics depending upon the maturity of their security infrastructure and availability of tools and technologies.*

e) <u>SOC Enrichments and Enhancements:</u> To determine the level of proactiveness of SOC in leveraging deployed technologies, automation of alert responses and deploying latest SOC technologies. This will help the SOC to evolve and ensure its preparedness in case of a future breach.

Table 34: Methodology to assess proactiveness of SOC

Sr. No.	Metric	Value(A)	Weightage (W)(%)	Weighted Score
1	**Dashboard and Analytics**			
1.1	Using Native technology dashboard	Yes=1, No=0	5	A×W
1.2	Custom developed dashboard	Yes=1, No=0	5	A×W
2	**Threat Hunting**			
2.1	Threat Hunting Exercise Carried out by:			
	Specialized Threat Hunting service provider	Yes=1, No=0	5	A×W
	Internal Team	Yes=1, No=0	3	A×W
2.2	Periodicity of the Exercise:			
	Quarterly	Yes=1, No=0	5	A×W
	Half-Yearly	Yes=1, No=0	3	A×W
2.3	Hypotheses:			
	Total no. of hypotheses [T]			
	No. of hypotheses based on the open vulnerabilities [X]		5	(X/T)×W
	No. of Hypotheses based on IoCs [Y]		5	(Y/T)×W
	No. of Hypotheses based on IoAs [Z]		5	(Z/T)×W
3	**Automation**			
3.1	Threat intel integration with SIEM	Yes=1, No=0	5	A×W
3.2	No. of SOAR actions triggered [T]			
	Total no. of different SOAR actions created [S]		5	(T/S)×W
4	**Technologies implemented**			
	Decoy	Yes=1, No=0	3	A×W

Sr. No.	Metric	Value(A)	Weightage (W)(%)	Weighted Score
	Sandboxing Solution	Yes=1, No=0	3	A×W
	UEBA	Yes=1, No=0	3	A×W
	Vulnerability Management Solution	Yes=1, No=0	3	A×W
	Encrypted Traffic Management	Yes=1, No=0	3	A×W
	DNS Security	Yes=1, No=0	3	A×W
	Intrusion prevention system	Yes=1, No=0	3	A×W
	Data classification solution	Yes=1, No=0	3	A×W
	Total		**75**	**E**

**The above metric for SOC operations is not exhaustive, REs are required to add other metrics depending upon the maturity of their cybersecurity infrastructure and availability of tools and technologies. 25% weightage is left for this to the REs.*

Annexure-O: Classification and Handling of Cybersecurity Incidents

A: Guidelines on Classification of Cybersecurity Incidents

Threshold for classifying incidents:

1. Any incident stated under CERT-In Cybersecurity directions[35] and meeting below criteria[36] shall be mandatorily reported within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents:
   i. Cyber incidents of severe nature (such as Denial of Service, Distributed Denial of Service, intrusion, spread of computer contaminant including Ransomware) on any part of the public information infrastructure including backbone network infrastructure
   ii. Data Breaches or Data Leaks
   iii. Large-scale or most frequent incidents such as intrusion into computer resource, websites etc.
   iv. Cyber incidents impacting safety of human beings

2. Cybersecurity incidents may be classified into the following four categories:
   i. Low Severity
   ii. Medium Severity
   iii. High Severity
   iv. Critical Severity

3. The parameters for classification of the incidents are as follows:

Table 35: Classification of cybersecurity incidents

Sr. No.	Category	Details
1	Low	System probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable; intelligence received regarding username password compromise; isolated instances of known malwares easily handled by antivirus software, etc.
2	Medium	Target recon or scans detected; penetration or Denial of Service attacks attempted with no impact on operations; widespread instances of known malwares easily handled by antivirus software; isolated instances of a new malwares not handled by anti-virus software; instances of phishing emails that were not recognized by employees and were clicked by them; instances of data corruption, modification and deletion being reported, etc.
3	High	Penetration or Denial of Service attacks attempted with limited impact on operations; widespread instances of a new malwares not handled by anti-virus software;

[35] Refer Annexure-I of Cert-IN direction No. 20(3)/2022 dated April 28, 2022
[36] Refer Q 30 in CERT-In Cybersecurity directions: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

		unauthorized access to servers and network devices; unauthorized or unexpected configuration changes on network devices detected; impersonation of SEBI officials in email communications; data exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.
4	Critical	Successful penetration or Denial of Service attacks detected with significant impact on operations; ransomware attack; exfiltration of market sensitive data; widespread instances of data corruption causing impact on operations; significant risk of negative financial or public relations impact, etc.

4. Any cyber incident that results in disruption, stoppage or variance in the normal functions/ operations of systems of the entity thereby impacting normal/ regular service delivery and functioning of the entity, must be classified as High or Critical incident.

B: Guidelines on Handling of Cybersecurity Incidents

1. Any cyber-attack(s), cybersecurity incident(s) and breach(es) experienced by REs falling under CERT-In Cybersecurity directions[37] shall be notified to SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. This information shall be shared to SEBI through the email ID ***mkt_incidents@sebi.gov.in*** within 6 hours and SEBI Incident Reporting Portal within 24 hours. Stock Brokers/ Depository Participants shall also report the incident(s) to Stock Exchanges/ Depositories along with SEBI and CERT-In within 6 hours of noticing/ detecting such incidents or being brought to notice about such incidents. Any/ all other cybersecurity incident(s) shall be reported to SEBI, CERT-In and NCIIPC (as applicable) within 24 hours. It may be noted that in case any RE does not report a cybersecurity incident to SEBI (when the RE is/ was aware of the incident) in a manner as laid down in the applicable cybersecurity framework, appropriate regulatory action may be taken by SEBI as deemed fit depending on the nature of the incident.

2. **Non-adherence to SOP:** Non-adherence to SOP would attract regulatory action as per the extant regulations for REs. The actions will be determined and taken as per the processes/ procedures laid down by SEBI.

3. Whenever a cybersecurity incident is reported[38] to SEBI by RE, the following steps need to be taken:
   3.1. The incident shall be reported on the SEBI Incident Reporting portal and on the email ID ***mkt_incidents@sebi.gov.in*** by the RE. The incident shall also be reported to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines/regulations/circular issued by CERT-In from time to time. Additionally, any entity whose systems have been identified as "Critical Information Infrastructure (CII)/ protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC), shall report and inform the incident to NCIIPC in a timely manner.

   3.2. During the life cycle of incident handling, the following aspects need to be broadly covered/captured:
      a. Whether the RE has followed the incident response plan of their organization while handling the incident.
      b. Whether the RE has taken necessary (immediate) measures to contain the incident impact.

[37] Refer Q 30 in CERT-In Cyber security directions: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf

[38] Cybersecurity incidents have to be reported by SEBI REs in accordance with the framework/circular/Standard Operating Procedure issued by SEBI.

c. Whether the RE has communicated to all relevant stakeholders about the incident.
d. Whether RE has taken sufficient measures to control, mitigate and remediate the incident.
e. Whether Root cause analysis (RCA) has been performed by RE.
f. Whether lessons learnt have been implemented by RE.
g. Whether the issues/loopholes identified in RCA stage have been addressed/plugged by the RE.
h. Whether RE has hired any independent agency to conduct IS Audit/ forensic audit related to the incident (as per applicability).
i. Whether RE has addressed/plugged vulnerabilities identified in the audit mentioned in point h above.

3.3. RE shall undertake the necessary activities and submit the relevant reports as per the following timelines:

Table 36: Timelines for post-cyber incident activity(ies) and report submission

Sr. No.	Name of the Report/ Activity	Timeline for Submission (from the date of reporting the incident or being brought to notice about the incident)
1	Interim Report*	3 Days
2	Mitigation measure	7 Days
3	Root Cause Analysis (RCA) report**	30 Days#
4	Forensic Audit Report (on the incident) and its closure report	Refer clause 3.4 below
5	Vulnerability Assessment and Penetration Testing (VAPT) for the incident and its closure reports	45 days
6	Any other report as required by SEBI	To be submitted as per SEBI direction

*The interim report must contain, inter alia, the following: Details of the incident including time of occurrence, information regarding affected processes/ systems/ network/ services, severity of the incident, and the steps taken to initiate the process of response and recovery.

**The RCA report shall inter-alia include exact cause of the incident (including root cause from vendor(s), if applicable), exact timeline and chronology of the incident, details of impacted processes/ systems network / services, details of corrective/ preventive measures taken (or to be taken) by the entity along with

timelines and any other aspect relevant to the incident. Additionally, it shall also include time when operations/ functions/ services were restored and in the event of a disaster, time when disaster was declared.

Additional time may be provided by SEBI for the submission of RCA on a case-by-case basis on request of the RE taking into account the complexity and nature of the incident(s). The same shall be an exception rather than the rule.

3.4. The RCA, forensic audit, VAPT reports, and closure reports shall be reviewed by the respective *IT Committee for REs* before the reports are submitted to SEBI. A report on the review conducted/ recommendations provided by *IT Committee for REs* shall also be submitted to SEBI along with the reports mentioned in Table 36.

3.5. SEBI shall examine the incident on the basis of reports submitted. Further, RE shall classify the cybersecurity incident based on its severity as per Table 35 and the same shall be reviewed by respective IT Committee for REs of the RE before the reports are submitted to SEBI.

3.6. In case the reports are found to be deficient or inaccurate in any manner (for instance no identification or incorrect identification of root cause, inaccurate sequence of events, etc.), appropriate regulatory action may be taken by SEBI. RE may be provided an additional time upto 15 days from the day of being notified of the deficiency/ inaccuracy, for submitting the accurate and complete report.

3.7. In the event of RE not submitting accurate and complete reports after being provided additional time, appropriate regulatory action may be taken by SEBI (over and above the action mentioned in clause 3.6 above).

3.8. Critical or High category of cybersecurity incidents experienced by MIIs, Qualified REs, and Mid-size REs shall be mandatorily put up for the review for HPSC-CS. Remaining incidents i.e., low and medium for all REs, and high and critical severity incidents for small-size and self-certification REs shall be processed by SEBI internally. The review by HPSC-CS and SEBI shall be as follows:

3.8.1. Review by HPSC-CS

i. For all the incidents placed before HPSC-CS, the committee may confirm the severity or may recommend a different severity on the basis of its analysis.

ii. The committee will examine the reports, review the severity of the incident and provide its recommendations on the same.

iii. Further, if the committee determines that the incident occurred on account of non-compliance of SEBI cybersecurity framework/ advisories, appropriate regulatory action may be taken by SEBI on the RE notwithstanding any action levied above.

iv. The recommendations of the committee shall be implemented by the RE in a time-bound manner. The timelines for the implementation shall be decided by the committee based on the discussion with relevant stakeholders (i.e. SEBI and the RE).

v. RE may be required to submit audit report(s) to verify the implementation of committee's recommendations.

3.8.2. Review by SEBI

i. If the matter is not required to be put up for the review of HPSC-CS, SEBI will examine the same (on the basis of the documents submitted by the RE).

ii. Further, if it is determined that the incident occurred on account of non-compliance of SEBI cybersecurity framework/ advisories, appropriate regulatory action may be taken by SEBI on the RE notwithstanding any action levied above.

iii. RE shall formulate a remediation and mitigation plan. The timelines for implementation of the measures shall also be decided based on the discussions (between SEBI and RE).

3.9. In case the recommendations are not implemented by the RE within the prescribed timeline, appropriate regulatory action may be taken by SEBI.

4. Forensic Investigation/ Audit

4.1. For all incidents classified as High or Critical, the RE shall submit a forensic audit/ investigation report.

4.2. For incidents classified as low or medium, forensic report shall be submitted if the RCA is inconclusive or if the SEBI/ HPSC-CS directs the same.

4.3. After the completion of forensic audit, RE shall submit a final closure report, which shall include the root cause of the incident, its impact and measures to prevent recurrence. The timeline for submission of the reports (including closure reports), shall be decided based on discussion with all stakeholders. However, the maximum period for the submission of forensic audit report shall be 75 days from date of reporting of incident.

In case the report is not submitted by the RE within the prescribed timeline, an appropriate regulatory action may be taken by SEBI.

4.4. For all the issues/ observations submitted in the forensic report, the RE shall provide a timeline for fixing the same. This timeline shall be submitted along with the forensic investigation/ audit report. Once the issues are resolved, the RE shall file a closure report for the same after review (of the report) by respective *IT Committee for REs*.

4.5. In case the issues are not fixed within the prescribed timeline, appropriate regulatory action may be taken by SEBI as deemed fit depending on the nature of incident.

Annexure-P: Reporting Format for Self-certification REs

REPORTING FORMAT FOR SELF-CERTIFICATION REs TO SUBMIT THEIR COMPLIANCE WITH APPLICABLE CSCRF PROVISIONS

NAME OF THE ORGANISATION: <Name>

ENTITY TYPE: <Intermediary Type>

ENTITY CATEGORY: <Category of the RE as per CSCRF>

RATIONALE FOR THE CATEGORY: <>

PERIOD: <>

RE's Authorised signatory declaration:

I/ We hereby confirm that implementation of all applicable CSCRF provisions have been verified by me/ us and I/ We shall take the responsibility and ownership of this self-certification.

Signature:

Name of the signatory:

Designation (choose whichever applicable): <MD/ CEO/ Board member/ Partners/ Proprietor>

Company stamp:

Annexures:

VAPT report as submitted by the auditor