SEBI's **Cybersecurity and Cyber Resilience Framework (CSCRF)** is the single graded standard for every SEBI-regulated entity — exchanges to self-certification REs. The implementation deadline has passed; the live obligation is now the recurring cyber-audit cycle. This summary gives a small or mid-size RE the operative picture on one desk reference: which circulars govern, where you fit in the five categories, what the controls demand, and the audit clock you are on. Full guide: vcisodesk.com/sebi-cscrf-implementation-guide-regulated-entities-india/.

The operative circular package (reading only the 2024 master gets you the wrong category)

Master circular: SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113, 20 Aug 2024 — five resilience goals: Anticipate · Withstand · Contain · Recover · Evolve.

As modified by: 31 Dec 2024 clarifications (scope fixes) · 28 Mar 2025 extension · **30 Apr 2025 clarifications (2025/60)** — revised thresholds, KRA→Qualified RE, broker dual-parameter rule, AIF manager-level aggregation, HSM mandate · 30 Jun 2025 extension + FAQs (2025/96) · **28 Aug 2025 technical clarifications (2025/119)** — DR RTO/RPO, ISO 27001 voluntariness, exclusivity principle, PM/Merchant Banker re-categorisation.

Deadline state: the 31 Aug 2025 implementation deadline has **passed** — no further blanket extension. Live checkpoints are the cyber-audit submissions: FY 2025-26 half-yearly reports were due 31 Mar 2026; the next cycle is due **30 Jun 2026**.

Newest development: 5 May 2026 SEBI advisory on AI-assisted vulnerability detection — advisory only; changes no deadline, threshold, or category.

1. Are you in scope?

In scope: MIIs (exchanges, clearing corporations, depositories) · stock brokers & DPs · AMCs · portfolio managers · AIFs · corporate investment advisers & research analysts · CRAs & debenture trustees · KRAs, RTAs, QRTAs.

Carved out: FPIs, FVCIs, individual investment advisers, LPCCs, QDPs, vault managers, REITs, InvITs. **Full exemption for small brokers:** fewer than 1,000 clients **and** under ₹1,000 crore annual trading volume — document the claim and re-check every FY; crossing either threshold flips you in.

2. The five categories — and the classification rules that trip firms up

Category	Who / what it demands
MIIs	Exchanges, CCs, depositories. Highest bar: own SOC, half-yearly audits, board cyber committee, ISO 27001 mandatory.
Qualified REs	Large REs by AUM/clients/volume; KRAs and Qualified Stock Brokers sit here. Near-MII requirements; flexible SOC sourcing; ISO 27001 recommended, not mandatory (28 Aug 2025).
Mid-size REs	Substantial controls, dedicated CISO function, structured IR. For portfolio managers this is the top category: AUM ≥ ₹10,000 cr (PMs have no Qualified tier).
Small-size REs	Reduced burden; may use the exchange-operated Market SOC (M-SOC). PMs: AUM > ₹3,000 cr and < ₹10,000 cr. Active merchant bankers land here.
Self-certification	Below small-size thresholds (PMs: ≤ ₹3,000 cr): self-certify on SEBI format. M-SOC waived for entities with fewer than 100 clients (per entity type); RTAs with <100 clients are exempt from SOC/M-SOC, not from CSCRF.

*Three 30 Apr 2025 rules that change self-categorisation: brokers take the **highest** category triggered by either client count or trading volume · AIF/VCF categorisation aggregates **all schemes at manager level** · multi-registration IAs follow their highest-triggered category. Category is set at FY start from prior-FY data and holds all year.*

3. Core obligations — what the auditor samples

- ☐ **G1 Governance:** board-level Technology Committee with cyber as standing agenda; designated CISO with documented authority; board-approved cyber crisis management plan. MIIs/Qualified REs: CISO at CTO/CIO level reporting to MD/CEO. Mid/Small/Self-cert REs may use a fractional or outsourced **vCISO** arrangement.
- ☐ **G2 SOC coverage:** MIIs in-house; Qualified/Mid-size via CERT-In-empanelled managed SOC or in-house; Small-size via **M-SOC**; self-cert REs <100 clients exempt. The SOC must ingest logs, correlate, run detections, and route alerts — a monthly PDF is not compliance.

- [ ] **G3 SBOM:** required at procurement for new core/critical software; for legacy critical systems, documented Board/Partners/Proprietor-approved rationale. Minimum fields: component inventory incl. transitive dependencies, supplier, version, licence, encryption details, hashes, update frequency.
- [ ] **G4 VAPT:** after every major release, by a CERT-In-empanelled IS auditing organisation. Closure SLAs: 3 months general; **1 week** for high-severity vulnerabilities arising from non-implementation of available patches.
- [ ] **G5 Data classification:** formal scheme (Public/Internal/Confidential/Restricted) tied to encryption, access management, and DLP for sensitive classes — applied to structured and unstructured data.
- [ ] **G6 Third-party risk:** vendor cybersecurity assessment; SLAs with security controls, audit rights, breach-notification clocks, exit clauses.
- [ ] **G7 HSM:** mandatory for MIIs and Qualified REs; Mid/Small/Self-cert may adopt documented, board-approved alternatives based on a risk assessment ("we use TLS" is not one).
- [ ] **G8 DR/BCP:** critical operations resume within **RTO 2 hours / RPO 15 minutes** (28 Aug 2025, IOSCO-aligned) — typically the most expensive technical line item; budget early.
- [ ] **G9 Incident reporting:** within **6 hours** of detection (inherited from CERT-In's 2022 Directions) to CERT-In and SEBI. Requires a tested IR plan, escalation matrix, forensic-readiness log retention, and RCA discipline.
- [ ] **G10 Cyber audit:** annual for most REs, **half-yearly for Qualified Stock Brokers**, by CERT-In-empanelled organisations; audits begin after the audit period ends; findings + ATRs filed with SEBI through the prescribed channel.

4. Twelve-month implementation arc (Mid/Small RE)

- [ ] **T1 Months 1–2:** confirm category against your entity-type thresholds; constitute/augment the Technology Committee; designate CISO (in-house or vCISO); board-approve the crisis plan.
- [ ] **T2 Months 3–4:** CERT-In-empanelled gap assessment; map controls to CSCRF; remediation roadmap with owners and budget; start data classification.
- [ ] **T3 Months 5–8:** stand up SOC/M-SOC; MFA, EDR, log aggregation, SIEM; SBOM for critical systems; VAPT on critical applications; encryption per classification; CSCRF-aligned vendor SLAs.
- [ ] **T4 Months 9–12:** IR tabletop; staff training; first empanelled cyber audit; SEBI filing; board posture review.
- [ ] **T5 Ongoing:** monthly management dashboard, quarterly Technology Committee, threat-intel ingestion, audit cadence, VAPT per release.

Indicative first-year budgets (assuming vCISO + managed SOC): Small-size REs ₹15–35 lakh, dropping to ₹10–18 lakh run-rate; Mid-size ₹40 lakh–₹1 crore depending on the gap. Indicative, not benchmarks.

5. If you remember five things

- [ ] **K1** Confirm your category from the 30 Apr 2025-modified threshold tables — and document the decision.
- [ ] **K2** Get the CISO designation, reporting line, and role description on paper, board-signed.
- [ ] **K3** Run an empanelled gap assessment before the auditor finds the gaps for you.
- [ ] **K4** Pick your SOC model (in-house / managed / M-SOC) and make the log integration real.
- [ ] **K5** If your audit finds material gaps: disclose with a credible remediation roadmap. A papered-over audit is the worst outcome — it surfaces later, with interest.

Content current as of 5 June 2026. SEBI touched CSCRF six times between Aug 2024 and May 2026 — verify thresholds against the latest circulars before relying on them. Full pillar guide: vcisodesk.com/sebi-cscrf-implementation-guide-regulated-entities-india/ — free, like everything on GRC RADAR.