AV Services
Linux Infrastructure Specialist since 1999

arun@avservices.in | +91 92205 60056
avservices.in | GSTIN: 27ACAPV2614B1Z0

SEBI CSCRF Linux Infrastructure
Gap Assessment Report

For SEBI-Regulated Entities · Prepared by AV Services

Mapped to SEBI CSCRF Circular dated August 20, 2024 and clarifications through April 2025

1. Purpose of This Report

SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF), effective August 2024, mandates that all regulated entities — stockbrokers, AMCs, depositories, registrar and transfer agents, portfolio managers, and research analysts — implement and audit specific cybersecurity controls across their IT infrastructure.

This report identifies the Linux-layer controls within CSCRF that are the direct responsibility of your infrastructure team, assesses typical gaps found in SME-scale regulated entities, and maps each gap to a remediation action that AV Services can deliver under a monthly retainer.

Audit coverage mandate: 100% of critical systems and 25% of non-critical systems must be covered in every CSCRF cyber audit cycle.

2. Which Entities Does This Apply To?

Entity Type	CSCRF Category	VAPT Frequency
Qualified Stock Brokers	Qualified RE	**Half-yearly**
Other Stockbrokers (>1,000 clients)	Mid-size or Small RE	Annual
AMCs, Depositories, RTAs	Qualified RE or MII	**Half-yearly**
Portfolio Managers, RAs	Self-certification RE	Annual
Brokers <1,000 clients, <₹1,000cr turnover	Self-certification (SOC exempt)	Annual

3. Patch Management — CSCRF Standard PR.MA

Requirement

High-severity patches must be applied within 1 week of release. All other patches within defined timelines. VAPT findings classified as high due to unpatched systems are treated as non-compliance. Patch compliance must be documented and audit-ready.

Common gaps found in SME-scale regulated entities

Servers running on default OS-shipped kernel versions 6-18 months behind current stable. No documented patch schedule. No evidence of patch testing before production deployment. Patch reports not maintained for auditor review.

AV Services remediation

Monthly patching window with pre-production testing. Patch compliance report generated after every cycle. Report format matches SEBI audit evidence requirements. Emergency patches applied within 24 hours of CERT-In advisory.

4. Access Control & Privilege Management — CSCRF Standard PR.AC

Requirement

Principle of least privilege enforced across all systems. Privileged access managed and reviewed. Root/sudo access documented. Terminated employee access revoked promptly. MFA on all admin interfaces. Zero-trust model applied to internal network access.

Common gaps

Shared root passwords still in use. SSH password authentication enabled. No audit trail of who accessed what and when. Former employees with active SSH keys discovered during audit. No formal access review process.

AV Services remediation

SSH hardening: key-based auth only, root login disabled. Individual named accounts for all admin access. Quarterly privileged access review with documented sign-off. Sudo rules tightened to task-specific permissions. Access revocation checklist triggered on HR notification.

5. Log Management & Audit Trails — CSCRF Standard DE.AE

Requirement

Logs must be collected from all sources: system, application, network, database, security, performance, and audit trail. Logs must be protected for integrity and confidentiality. Minimum 1-year retention. Logs must be available for SEBI on demand.

Common gaps

Logs stored only locally on the same server being audited — no separation. Log rotation set to 7 or 30 days. No centralised log aggregation. Audit trail for privileged user actions absent. Log files writable by application users.

AV Services remediation

Centralised log aggregation to a separate secured log server. Immutable log storage with integrity verification. 1-year retention configured and monitored. Monthly log review with anomaly escalation. Audit trail for all sudo/root actions via auditd.

6. Incident Response — CSCRF Standard RS

Requirement

Documented incident response plan, tested annually. Cyber incidents reported to SEBI and CERT-In within 6 hours. Root Cause Analysis report produced post-incident. Recovery procedures documented and drilled.

Common gaps

No written incident response plan specific to Linux infrastructure. No escalation matrix. No RCA template. Incident reports produced ad hoc, inconsistent format, not audit-ready.

AV Services remediation

AV Services Incident Response SLA provides 24/7 emergency response — remote within 2 hours, onsite Mumbai within 4 hours. RCA report provided within 48 hours in SEBI-compatible format. Incident response plan drafted as part of onboarding. Annual tabletop drill included in Business Critical retainer tier.

7. Backup & Disaster Recovery — CSCRF Standard RC

Requirement

Backup and recovery procedures documented. Recovery tested periodically. RTO and RPO defined. Data sovereignty: data stored within India.

Common gaps

Backups running but never tested for restore. No documented RTO/RPO. Backup to cloud storage outside India without data residency verification. No monitoring — backup failures silent for weeks.

AV Services remediation

Automated backup with monitoring and alerting. Monthly restore test with documented proof. RTO/RPO defined and tested. India-based storage verified. Backup reports included in monthly retainer report.

8. Security Hardening — CSCRF Standard PR.IP / PR.PT

Requirement

Systems hardened against known attack vectors. Network segmentation in place. Unnecessary services and ports disabled. CIS Benchmark or equivalent applied to critical systems.

Common gaps

Default OS install with no hardening. Unnecessary services running (telnet, FTP, rpcbind). No network segmentation between trading and back-office systems. World-readable config files containing credentials.

AV Services remediation

CIS Benchmark hardening applied to all servers. Firewall rules reviewed and locked down. Unnecessary services disabled. Network segmentation design reviewed. Hardening report produced for auditor.

9. AV Services Retainer — CSCRF Control Coverage

CSCRF Control Area	Retainer Tier	Covered
Monthly patching + patch compliance report	All tiers	✓
Access control hardening + quarterly review	All tiers	✓
Log aggregation + 1-year retention	Professional & above	✓
Monthly log review + anomaly escalation	Professional & above	✓
24/7 emergency incident response	All tiers	✓
RCA report post-incident	All tiers	✓
Backup monitoring + monthly restore test	All tiers	✓
CIS hardening + hardening report	Business Critical	✓
Annual incident response plan + drill	Business Critical	✓

Start with a free 30-minute audit

We assess your current Linux infrastructure against SEBI CSCRF requirements and identify your top 3 gaps — at no cost, no obligation.

avservices.in/free-audit/

+91 92205 60056 · arun@avservices.in