SEBI CSCRF Checklist

17 controls from SEBI Cyber Security & Cyber Resilience Framework

SEBI CSCRF

GOVERNANCE

- [ ] Board-approved Cyber Security Policy reviewed within last 12 months
- [ ] Designated CISO with documented role, mandate, and reporting line
- [ ] Cyber Security Committee constituted with cross-functional membership
- [ ] Annual cyber security audit conducted by CERT-In empanelled auditor

TECHNICAL CONTROLS

- [ ] Network segmentation implemented between critical and non-critical zones
- [ ] IDS/IPS deployed and monitored at network perimeter and critical segments
- [ ] Web Application Firewall (WAF) deployed for all internet-facing applications
- [ ] Multi-factor authentication enforced for all privileged and remote access
- [ ] Annual access review completed for all critical systems and applications
- [ ] Critical security patches applied within 30 days of release

INCIDENT RESPONSE

- [ ] Incident response plan documented with roles, escalation, and communication
- [ ] Tabletop exercise conducted within last 12 months with documented findings
- [ ] 6-hour SEBI incident reporting mechanism tested and operational
- [ ] Post-incident review process documented with lessons-learned integration

THIRD-PARTY RISK

- [ ] Security due diligence completed for all critical third-party vendors
- [ ] Contractual security requirements documented in all vendor agreements
- [ ] Annual vendor security review programme operational with risk scoring

SCORING GUIDE

15-17	11-14	7-10	<7
Audit-ready	Functional gaps	Material remediation	Escalate

Automate this checklist >> practitioner-toolkit.creativecyber.in