CREST Accredited

certin Empanelled

A COMPLIANCE READINESS RESOURCE

SEBI Advisory Readiness Checklist

A practical mapping of SEBI Circular dated 05 May 2026 to auditable items for Regulated Entities and empaneled vendors.

BriskInfosec™

VULNERABILITY TO VICTORY

CONTENTS

What you'll find inside

ABOUT THIS CHECKLIST

A working document for your audit cycle

On 05 May 2026, SEBI issued an advisory (ref: HO/13/19/12(1)2026-ITD-1) addressing emerging cybersecurity risks from advanced AI vulnerability detection tools, citing Claude Mythos specifically. The advisory does not replace the Cyber Security and Cyber Resilience Framework (CSCRF). It adds ten operational controls that Regulated Entities and their empaneled vendors must demonstrate in their next audit cycle.

This document translates each of those ten controls into specific, auditable line items with evidence requirements. It is designed for use by Chief Information Security Officers, Chief Compliance Officers, IT committee members, and the security teams who support them.

HOW TO USE THIS DOCUMENT

Five steps

1 **Read the background section**

Understand what changed and why your next audit scope is now wider.

2 **Walk through each of the 10 control areas**

For each item, mark your current status: Compliant, Partial, Gap, or Not Applicable.

3 **Note the evidence available**

Auditors will ask for documentary evidence. If you cannot point to a document, the control is a Gap.

4 **Score using the readiness worksheet**

Calculate your overall readiness percentage and identify priority gaps.

5 **Decide your remediation timeline**

Plan remediation ahead of your audit window, not during it.

BACKGROUND

SEBI Circular dated 05 May 2026

Why SEBI issued this advisory

The rapid evolution of AI-driven vulnerability identification tools (Claude Mythos is named specifically in the advisory) has introduced new dimensions of cyber risk for Regulated Entities. Such tools can identify and potentially exploit existing vulnerabilities at speed and scale. They also raise concerns around data confidentiality, application integrity, and the reliability of outputs from AI-driven processes.

Because the securities market ecosystem is interconnected and interdependent, SEBI judged that a coordinated approach to vulnerability management, information sharing, and monitoring was required to prevent cascading impact across market participants.

The cyber-suraksha.ai task force

SEBI has constituted a task force (project-cyber-suraksha.ai@sebi.gov.in) comprising representatives from MIIs, QRTAs, all QREs, and other related stakeholders with a four-part mandate: examine AI cybersecurity risks and devise a uniform mitigation strategy; share threat intelligence and best practices; report cyber incidents and vulnerabilities on a priority basis; and review the cyber posture of third-party application service providers including empaneled vendors.

Who must comply

The advisory addresses every category of SEBI-regulated entity, including: Alternative Investment Funds, Bankers to an Issue, Self-Certified Syndicate Banks, Clearing Corporations, Collective Investment Schemes, Credit Rating Agencies, Custodians, Debenture Trustees, Depositories, Designated Depository Participants, Investment Advisors, Research Analysts, KYC Registration Agencies, Merchant Bankers, Mutual Funds and AMCs, Portfolio Managers, Registrars and Share Transfer Agents, Stock Brokers, Stock Exchanges, and Venture Capital Funds.

> **READ TOGETHER WITH**
> This advisory must be read together with SEBI's Cyber Security and Cyber Resilience Framework (CSCRF) and any subsequent updates SEBI issues. The advisory adds to existing obligations — it does not replace them.

FRAMEWORK

Self-assessment scoring

For each checklist item, assign one of four status values. Use the scoring weights to calculate overall readiness in the summary worksheet at the end of this document.

Status	Definition	Score
Compliant	Control is fully implemented, evidence is documented and current (within the last audit cycle), and processes are operating as designed.	**1.0**
Partial	Control is partially implemented or implemented but evidence is incomplete, outdated, or inconsistent. Gap can be closed with minor remediation.	**0.5**
Gap	Control is not implemented, or implementation is so limited that audit failure is likely. Requires substantive remediation work.	**0.0**
N/A	Control does not apply to this entity (e.g., M-SOC onboarding for entities not yet eligible). Excluded from scoring denominator.	—

Calculating overall readiness

Readiness score (%) = (Sum of item scores) ÷ (Total applicable items) × 100

Interpreting your score

Range	Posture	Recommended action
85-100%	**Audit-ready**	Strong posture. Focus on continuous improvement and emerging AI threat vectors.
65-84%	**Largely ready**	Gaps are addressable. Plan remediation 60-90 days ahead of your audit window.
45-64%	**Material gaps**	Significant remediation required. Prioritise the highest-weighted controls.
0-44%	**Substantial risk**	Audit failure likely without urgent intervention. Consider engaging external support.

CONTROL 1

Patching and Vulnerability Mitigation

SEBI Advisory Annexure-A, Point 1

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
1.1	Documented patch management policy exists, covering OS, applications, firmware, and network devices. *Evidence: Approved policy document with version control and last review date*				
1.2	Inventory of all systems with current patch level is maintained and updated at least monthly. *Evidence: Patch inventory report from CMDB or patch management tool*				
1.3	Critical and high-severity vendor patches are applied within defined SLA (typically 7–30 days of release). *Evidence: Patch deployment logs with timestamps and SLA tracking dashboard*				
1.4	Process exists for emergency out-of-cycle patching when critical vulnerabilities are disclosed. *Evidence: Emergency patch SOP and at least one recent invocation log*				
1.5	Compensating controls are applied for vulnerabilities where a vendor patch is delayed or unavailable. *Evidence: Documented compensating controls (e.g. virtual patching, network segmentation, access restriction) with risk acceptance record*				
1.6	Patch testing process exists in a non-production environment before production rollout. *Evidence: Change management records showing test → UAT → prod progression*				
1.7	Rollback procedures are documented and tested for patches that cause issues. *Evidence: Rollback playbook and at least one tested rollback event*				
1.8	Independent verification confirms patches are actually applied (not just scheduled). *Evidence: Compliance scan reports from independent tool, not from patch management system*				

CONTROL 2

Vulnerability Assessment and Security Audits

SEBI Advisory Annexure-A, Point 2 · CSCRF

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
2.1	Regular vulnerability scanning is conducted across all in-scope assets at defined frequency (typically weekly to monthly). *Evidence: Scan schedule and last 12 months of scan reports*				
2.2	Both authenticated and unauthenticated scans are performed where applicable. *Evidence: Scan configuration showing credentialed scan policies*				
2.3	AI-assisted vulnerability assessment tools have been evaluated for suitability within audit programme. *Evidence: Tool evaluation document, vendor assessments, or POC results*				
2.4	Annual VAPT is conducted by a CERT-In empanelled auditor for all internet-facing and critical internal applications. *Evidence: Signed VAPT report from CERT-In empanelled firm within last 12 months*				
2.5	VAPT scope explicitly covers web applications, mobile applications, APIs, network infrastructure, and cloud environments. *Evidence: Scope document attached to VAPT engagement letter*				
2.6	Critical and high findings from VAPT and scans are remediated within defined SLA (typically 30–90 days). *Evidence: Remediation tracking with finding status and closure dates*				
2.7	Retest is conducted after remediation to verify closure of findings. *Evidence: Retest report or addendum to original VAPT*				
2.8	Vulnerability management programme integrates threat intelligence to prioritise patching by exploitability. *Evidence: Threat intel feed subscriptions and prioritisation methodology document*				
2.9	Findings reports are reviewed by the IT committee or designated governance body. *Evidence: Meeting minutes referencing VAPT findings within last reporting period*				

CONTROL 3

Third-Party Vendor Risk Management

SEBI Advisory Annexure-A, Point 3

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
3.1	Complete inventory of all third-party application service providers and empaneled vendors is maintained. *Evidence: Vendor master list with criticality classification*				
3.2	Each critical vendor has undergone documented security risk assessment within last 12 months. *Evidence: Vendor risk assessment reports filed by procurement or risk team*				
3.3	Vendor contracts include security obligations, audit rights, and incident notification requirements. *Evidence: Sample contracts with security schedules / DPAs*				
3.4	Empaneled COTS vendors have been formally directed to assess AI-led vulnerability detection risks. *Evidence: Written communication to vendors referencing SEBI advisory and required assessment*				
3.5	Vendor responses regarding patch timeliness, VAPT cadence, and continuous monitoring have been received and reviewed. *Evidence: Vendor attestation responses and review summary*				
3.6	Process exists to verify vendor security claims (not just accept attestations). *Evidence: Vendor audit programme or SOC 2 / ISO 27001 verification process*				
3.7	Hardening measures applied by vendors are documented and reviewed periodically. *Evidence: Vendor hardening attestation or configuration review report*				
3.8	Exit and transition plans exist for critical vendor relationships to manage concentration risk. *Evidence: Documented exit strategy for at least top 3 critical vendors*				

CONTROL 4

Change Management

SEBI Advisory Annexure-A, Point 4

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
4.1	Documented change management policy exists and is approved by senior management. *Evidence: Approved policy with version history and effective date*				
4.2	All changes — including minor changes — are recorded in a change management system. *Evidence: Sample CR records showing minor and emergency change documentation*				
4.3	Each change record includes impact analysis covering security, availability, and dependencies. *Evidence: Sample impact analysis sections from recent CRs*				
4.4	Changes are reviewed and approved by Change Advisory Board (CAB) or equivalent before implementation. *Evidence: CAB meeting minutes with change approvals*				
4.5	Testing in a non-production environment is mandatory and documented for all non-emergency changes. *Evidence: Test results attached to CR records*				
4.6	Production deployment follows documented secure deployment procedures. *Evidence: Deployment runbooks and access controls during deployment windows*				
4.7	Post-implementation review is conducted for significant changes. *Evidence: PIR documents showing outcomes vs expected results*				
4.8	Emergency change process exists with retrospective documentation and CAB review. *Evidence: Emergency change SOP and at least one retrospective review*				

CONTROL 5

API Security

SEBI Advisory Annexure-A, Point 5

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
5.1	Comprehensive inventory of all APIs (internal, external, partner) is maintained and updated within last 90 days. *Evidence: API inventory document or API gateway export*				
5.2	Each API is mapped to its consuming applications and business owners. *Evidence: API-to-application mapping in inventory*				
5.3	Strong authentication is implemented on all production APIs (OAuth 2.0, mTLS, or equivalent). *Evidence: Authentication configuration in API gateway and sample API specifications*				
5.4	Authorisation enforces least privilege based on end-user identity, not just service identity. *Evidence: RBAC/ABAC policies and access control test results*				
5.5	Rate limiting and abuse detection are configured on public-facing APIs, with thresholds documented and alerting verified. *Evidence: API gateway rate limit configuration plus threshold documentation and a recent alert or incident record*				
5.6	API whitelist-based connection policy is documented and enforced at the gateway level. *Evidence: Whitelist configuration and exception approval log*				
5.7	API security testing is included as a discrete scope item in last VAPT cycle. *Evidence: API security findings section in latest VAPT report*				
5.8	Sensitive data exposure via API responses is reviewed and minimised (e.g., no PAN, no full account numbers). *Evidence: API data classification document and DLP scan results*				
5.9	API logging captures sufficient detail for forensic investigation and is retained per policy. *Evidence: Sample API logs and log retention policy document*				

CONTROL 6

SOC Monitoring and M-SOC Onboarding

SEBI Advisory Annexure-A, Point 6

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
6.1	24x7 security monitoring is in place, either internally, via MSSP, or via M-SOC. *Evidence: SOC operating model document and staffing roster*				
6.2	SIEM solution ingests logs from all critical systems including network, endpoint, application, and cloud. *Evidence: SIEM log source inventory and ingestion health report*				
6.3	Detection rules cover known attack patterns including those in MITRE ATT&CK; framework. *Evidence: Rule inventory mapped to ATT&CK; techniques*				
6.4	Low-priority alerts are reviewed regularly — not only high-priority alerts. *Evidence: Alert triage SOP and sample weekly review records*				
6.5	Where SOAR is deployed, playbooks are tested before production use and integrated with the SIEM. (Mark N/A if SOAR is not in use.) *Evidence: Playbook inventory, testing/validation sign-off, and recent execution logs*				
6.6	Onboarding to Market SOC (M-SOC) operated by NSE and BSE has been initiated for eligible entities. *Evidence: M-SOC onboarding correspondence and integration milestone tracker*				
6.7	Where M-SOC onboarding is complete, integration is functioning and threat alerts are being received. *Evidence: M-SOC integration confirmation and recent alert flow evidence*				
6.8	Awareness and handholding sessions with M-SOC have been attended by relevant team members. *Evidence: Training attendance records*				
6.9	SOC metrics (MTTD, MTTR, alert volume, false positive rate) are tracked and reported to leadership. *Evidence: Monthly SOC metrics report*				

CONTROL 7

Risk Assessment

SEBI Advisory Annexure-A, Point 7 · CSCRF

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
7.1	Periodic cyber risk assessment is conducted at frequency mandated by CSCRF for entity category. *Evidence: Risk assessment report from last 12 months*				
7.2	Risk assessment explicitly covers third-party service providers, not only internal systems. *Evidence: Vendor risk inclusion in latest assessment scope*				
7.3	Scenario-based testing is included, covering both internal and external risk scenarios. *Evidence: Scenario library and test execution records*				
7.4	AI-based model capability is included as a defined risk scenario. *Evidence: AI scenario documentation referencing Mythos-class capabilities*				
7.5	Risk register is maintained with owners, scores, treatment plans, and review dates. *Evidence: Current risk register export*				
7.6	Risk treatment decisions (accept, mitigate, transfer, avoid) are documented and approved by appropriate authority. *Evidence: Risk treatment approval records*				
7.7	Inherent and residual risk are both calculated and tracked. *Evidence: Risk register showing both ratings per risk*				
7.8	Risk assessment results are reported to the Board or IT committee. *Evidence: Board / IT committee meeting minutes referencing risk assessment*				

CONTROL 8

System Hardening

SEBI Advisory Annexure-A, Point 8

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
8.1	Hardening baselines exist for all OS, database, network device, and application categories. *Evidence: Approved hardening standards documents*				
8.2	Hardening baselines align with industry standards (CIS Benchmarks, DISA STIGs, or equivalent). *Evidence: Cross-reference between internal standards and external benchmarks*				
8.3	Default accounts and credentials have been disabled or changed on all production systems. *Evidence: Configuration audit results confirming no default credentials*				
8.4	Unnecessary services, ports, and protocols have been disabled on production systems. *Evidence: Port/service audit reports*				
8.5	Least privilege is enforced through role-based access controls across systems and applications. *Evidence: RBAC matrix and access review records*				
8.6	Zero Trust Network Access (ZTNA) is deployed for remote access and lateral movement controls. *Evidence: ZTNA architecture documentation and rollout status*				
8.7	Privileged access is controlled, logged, and periodically reviewed, with session monitoring for sensitive systems. *Evidence: Privileged access register, session/activity logs, and periodic access review records*				
8.8	Hardening compliance is verified by automated tools at defined frequency. *Evidence: Compliance scan reports from CIS-CAT or equivalent*				
8.9	Drift from hardening baseline triggers alerts and remediation workflow. *Evidence: Drift detection rules and recent remediation tickets*				

CONTROL 9

Asset Inventory and Software Bill of Materials

SEBI Advisory Annexure-A, Point 9

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
9.1	Comprehensive asset inventory is maintained covering hardware, software, cloud resources, and data. *Evidence: Asset inventory export from CMDB with last update timestamp*				
9.2	Asset inventory is updated at defined frequency (at least quarterly, ideally continuous). *Evidence: Update logs or automated discovery configuration*				
9.3	Each asset has assigned owner, criticality rating, and data classification. *Evidence: Asset record sample fields*				
9.4	Software Bill of Materials (SBOM) is maintained for all critical applications, ideally in a standard format (SPDX or CycloneDX). *Evidence: SBOM documents for top critical applications*				
9.5	SBOM covers open-source dependencies, including transitive dependencies. *Evidence: Sample SBOM showing direct + transitive components*				
9.6	SBOM is monitored for newly disclosed vulnerabilities in listed components. *Evidence: Vulnerability matching reports against SBOM*				
9.7	Process exists to update SBOM whenever application code or dependencies change. *Evidence: SDLC integration documentation showing SBOM generation in CI/CD*				

CONTROL 10

IT Committee Guidance and Long-Term AI Plan

SEBI Advisory Annexure-A, Point 10

#	Audit item / Evidence required	Compl.	Partial	Gap	N/A
10.1	IT committee has reviewed the SEBI advisory of 05 May 2026 and minuted its discussion. *Evidence: IT committee meeting minutes referencing the advisory*				
10.2	IT committee has provided documented guidance on mitigating risks from AI-led vulnerability detection models. *Evidence: Documented guidance, charter additions, or risk register updates*				
10.3	A long-term plan exists for the use of AI in vulnerability detection and remediation. *Evidence: Strategy document with timeline and milestones*				
10.4	The long-term plan addresses autonomous and agentic mitigation capabilities, not only detection. *Evidence: Strategy sections explicitly covering agentic AI use cases*				
10.5	Risk recalibration has been performed to account for AI-accelerated threat scenarios. *Evidence: Updated risk register showing AI-related risks*				

SEBI Task Force: cyber-suraksha.ai

SEBI has constituted the cyber-suraksha.ai task force (project-cyber-suraksha.ai@sebi.gov.in) comprising representatives from MIIs, QRTAs, QREs, and related stakeholders. Its mandate covers examining AI cybersecurity risks, sharing threat intelligence, and reviewing third-party vendor security posture across the securities market ecosystem.

WORKSHEET

Readiness summary

After completing the assessment for each control area, transfer your counts to this worksheet to calculate overall readiness.

Control area	Total items	Compliant	Partial	Gap	N/A	Score
1. Patching and Vulnerability Mitigation	**8**	___	___	___	___	_____
2. Vulnerability Assessment and Audits	**9**	___	___	___	___	_____
3. Third-Party Vendor Risk Management	**8**	___	___	___	___	_____
4. Change Management	**8**	___	___	___	___	_____
5. API Security	**9**	___	___	___	___	_____
6. SOC Monitoring and M-SOC	**9**	___	___	___	___	_____
7. Risk Assessment	**8**	___	___	___	___	_____
8. System Hardening	**9**	___	___	___	___	_____
9. Asset Inventory and SBOM	**8**	___	___	___	___	_____
10. IT Committee and AI Plan	**5**	___	___	___	___	_____
TOTAL	**81**	___	___	___	___	_____

CALCULATE YOUR READINESS SCORE

Score per item: Compliant = 1.0, Partial = 0.5, Gap = 0.0, N/A = excluded

Numerator = (Compliant count × 1.0) + (Partial count × 0.5)
Denominator = Total items – N/A items
Readiness % = (Numerator ÷ Denominator) × 100

YOUR OVERALL READINESS _____ %

NEXT STEPS

What to do once you've scored

01 **Document your gaps**
For every item marked Partial or Gap, write a one-line remediation action with an owner and target date. A gap without an owner and a date is not a remediation plan.

02 **Prioritise by exposure, not by control number**
A single Gap in API security or M-SOC monitoring carries more audit and operational risk than several Gaps in lower-impact controls. Address the controls that protect customer-facing systems first.

03 **Map remediation to your audit window**
Work backward from your next CSCRF audit. Allow at least 60 days for evidence to accumulate after a control is implemented — auditors look for sustained operation, not point-in-time fixes.

04 **Engage your IT committee early**
Annexure point 10 explicitly routes through your IT committee. Bring this checklist to the next meeting and secure formal endorsement of the remediation plan.

05 **Document the journey, not just the destination**
Auditors increasingly value evidence of continuous improvement. Keep records of when each control moved from Gap to Partial to Compliant.

Important notice. This checklist is a working document prepared by Briskinfosec to assist Regulated Entities and empaneled vendors in interpreting SEBI Circular HO/13/19/12(1)2026-ITD-1 dated 05 May 2026. It does not constitute legal, regulatory, or audit advice, and it is not a substitute for a formal audit conducted by a CERT-In empanelled auditor. Specific compliance obligations vary by entity category and should be confirmed against the underlying SEBI circular, the Cyber Security and Cyber Resilience Framework, and any subsequent updates issued by SEBI.