CERT-In Compliance & Implementation Report

Target system: commercial security product with server infrastructure, cloud services, admin dashboards, mobile clients, and IoT/edge cameras (real-time audio/video, telemetry, AI).
Prepared: for product/security engineering, compliance, and SOC teams.

Executive summary (top takeaways)

1. **Immediate obligations:** CERT-In Directions require certain cyber incidents to be reported to CERT-In within **6 hours** of noticing them. You must have a SOC / POC and IR SOP able to support that timeline. CERT-In+1
2. **Logging & data locality:** Maintain ICT system logs for a rolling **180 days**, with the ability to provide logs to CERT-In; CERT-In expects logs to be available within India. azb+1
3. **Operational readiness & auditability:** CERT-In now emphasizes auditability, SBOM/CBOM practices, and more prescriptive audit policy guidance (CERT-In audit policy guidance / SBOM guidance). You must embed SBOM/firmware BOM, supply-chain controls, and be audit-ready. CERT-In+1

1. Which CERT-In rules / guidance apply to your product

- **Directions under section 70B (28 Apr 2022):** mandatory incident reporting timelines, POC, log retention, cooperation with CERT-In orders. Applicable to service providers, intermediaries, data centres, body corporates (broadly covers commercial vendors and cloud/hosting providers). CERT-In
- **FAQs on the Directions:** clarifies scope, timelines, formats for reporting, and expectations on what should be reported within 6 hours. CERT-In

- **CERT-In Security Guidelines (SBOM/CBOM/AIBOM/HBOM, 2024):** technical requirements for software/firmware bills of materials and supply chain transparency. Useful for product SBOM and third-party components. CERT-In
- **Comprehensive Cyber Security Audit Policy Guidelines (CERT-In, July 25, 2025):** the audit policy that standardizes audit scope, frequency and the role of empanelled auditors — important for internal audit planning and vendor contracts. CERT-In

2. Mandatory operational requirements (what you must do) — plain language + evidence

1. **Report specified cyber incidents within 6 hours** of noticing them (or being notified). If full details are not available within 6 hours, provide the available information and update CERT-In later. (TIMELINE = 6 hours). CERT-In+1
2. **Maintain logs/telemetry for 180 days** (rolling) and be able to furnish them to CERT-In on request; logs should be retained within India (or a copy retained within India) to meet CERT-In directions. azb+1
3. **Appoint and maintain an up-to-date POC** (24×7 contact details) to interface with CERT-In; the POC must be able to act on CERT-In directions quickly. CERT-In
4. **Comply with CERT-In orders/directions** for mitigation actions, including providing information (up to near–real-time) and taking protective steps as directed. Non-compliance may attract penalties. CERT-In
5. **Ensure secure time synchronization** (NTP/time source) so logs have authoritative timestamps (CERT-In notes time-source fidelity expectation). CERT-In
6. **Publish & maintain SBOM / firmware BOM information** per CERT-In technical guidelines to improve supply-chain transparency and vulnerability response. CERT-In
7. **Prepare for mandatory audits** under the Comprehensive Cyber Security Audit Policy (audit frequency, scope and empanelled auditors), especially once the product is used by large enterprises or critical infrastructure customers. CERT-In

3. How these apply to the components of your product (technical mapping + required controls)

A. Servers & Cloud back-end

- **Incident detection & reporting:** SOC must detect applicable incidents (see Annex I of Directions) and be able to deliver an initial incident report to CERT-In within 6 hours. Implement automated alerting and a fast escalation path to the CERT-In POC. CERT-In
- **Logging:** centralize logs (auth, API gateway, WAF, stream servers, DB access, admin actions) into a SIEM; maintain retention (180 days) with in-India storage or an India-resident copy. Ensure logs include user/device identifiers and are tamper-evident (WORM or signed logs). CERT-In
- **Time sync:** all servers must sync to approved NTP sources (no significant drift) so logs are forensically useful. CERT-In

B. Host devices / Mobile apps

- **POC capability:** mobile app vendor must provide emergency contact and be ready to remediate or disable compromised app builds or revoke keys. CERT-In
- **Client telemetry:** design client to log security-relevant events (auth failures, config changes, OTA updates) and ship them securely to the SIEM while preserving PII rules.

C. IoT / Edge devices (cameras, ESP32 class hardware)

- **Firmware SBOM & signing:** maintain firmware SBOM and sign all firmware updates; provide a verifiable chain for each firmware build (SBOM + cryptographic signatures). CERT-In SBOM guidance is explicit on CBOM/SBOM practices. CERT-In
- **Local logs & remote telemetry:** devices should retain critical event logs locally and forward them to central servers; ensure logs are available for 180 days (or forwarded and retained centrally). CERT-In
- **Secure update & rollback protection:** OTA update mechanism must verify signatures, prevent downgrade/rollback exploitation, and record update events for audit.

D. Supply chain & third-party libraries

- **SBOM/CBOM for software & firmware:** produce SBOMs for all components (open source and commercial) and keep them current per CERT-In technical guidance. This supports fast vulnerability triage after public CVE disclosures. CERT-In
- **Vendor due diligence & contracts:** add contractual clauses for rapid cooperation with CERT-In requests and for 24×7 POC availability; ensure vendors retain logs and can produce SBOMs/audit artifacts.

4. Incident reporting — what to prepare in your SOC now

- **IR SOP & 6-hour playbook:** create a "6-hour report" playbook: essential fields (time of occurrence, affected systems, indicators of compromise, immediate containment steps, contact info). Use CERT-In reporting format available on their site. Initial report can be partial; follow up with full forensic report. CERT-In+1
- **Evidence preservation:** implement tools to collect memory, disk, packet captures and preserve chain-of-custody for any device or server involved. Ensure logs are WORM or cryptographically protected to prevent tampering. CERT-In
- **POC staffing and redundancy:** appoint primary + alternate POC; ensure 24×7 availability and test contactability regularly. CERT-In

5. Logging & retention (technical checklist)

- Central SIEM for: auth logs, API/gateway logs, WAF, DB access, OTA update events, device heartbeats.
- Retention: **180 days** (rolling). Ensure backups of logs and a tested retrieval process. CERT-In
- Logs stored / accessible in India (or copy residing in India) — verify cloud region and data residency settings for AWS/GCP/Azure. CERT-In
- Timestamps: NTP sync, time source compliance. CERT-In

6. SBOM, firmware / supply chain transparency (practical steps)

- **SBOM generation:** integrate SBOM generation into CI/CD (e.g., cyclonedx / SPDX outputs) for server code, mobile apps, native libs, and firmware builds. Maintain versioned SBOMs per build. CERT-In
- **CBOM for cloud & AI:** document model artifacts and third-party AI libs (AIBOM) and host model checksums. CERT-In
- **Publish & escrow:** keep SBOMs internally and provide them to customers or CERT-In upon request per policy.

7. Audit readiness & CERT-In empanelled audits

- **Comprehensive Cyber Security Audit Policy (CERT-In):** expect more prescriptive audits and readiness checks, including OT/IoT scopes and evidence of controls. Maintain an audit pack (policies, logs, SBOMs, test results, pentest reports) for auditors. CERT-In
- **Internal cadence:** run quarterly internal compliance reviews and annual third-party audits (or more frequently if required by customers/regulators). CERT-In

8. Contractual & customer-facing obligations

- Include clauses for:
    - 24×7 POC and incident escalation timelines
    - Obligation to cooperate with CERT-In investigations and to comply with lawful orders
    - Log retention and location guarantees (India region agreement)
    - SBOM delivery and vulnerability disclosure processes

9. Implementation roadmap (90/180/365 day plan)

0–90 days

- Create IR SOP and 6-hour report template. CERT-In
- Appoint POC + test CERT-In contactability. CERT-In
- Centralize logging, implement NTP sync, start 180-day retention. CERT-In

90–180 days

- Integrate SBOM generation into CI/CD for server, client and firmware builds. CERT-In
- Harden OTA update pipeline and firmware signing.
- Conduct internal audit and tabletop IR drills (simulate 6-hour reporting).

180–365 days

- Engage third-party audit (CERT-In empanelled auditor if required) per Comprehensive Audit Policy. CERT-In
- Complete supply chain due diligence and vendor agreements with CERT-In cooperation clauses.

10. Example SOC playbook snippets (for the 6-hour report)

- **Trigger:** detection of data exfiltration, ransomware, unauthorized access, system compromise, targeted scanning of critical infrastructure (Annex I incidents). CERT-In
- **Action within 0–1 hour:** validate incident, capture volatile data, isolate affected hosts/services, escalate to IR lead.
- **Action within 1–3 hours:** prepare initial incident pack (affected assets, impact estimate, IOCs), notify POC and leadership.
- **Action within 3–6 hours:** submit initial CERT-In report (minimum required fields); continue containment and evidence collection. CERT-In

11. Risk & compliance checklist (quick)

- 6-hour reporting playbook & practice drills. CERT-In
- Appointed 24×7 POC (details registered/maintained). CERT-In
- Centralized SIEM & 180-day logs (India residency or copy). CERT-In
- NTP sync & signed/tamper-evident logs. CERT-In
- SBOM/CBOM/AIBOM processes integrated into CI/CD. CERT-In
- Firmware signing, OTA safety & rollback protection. CERT-In
- Vendor contracts / SLAs updated for CERT-In cooperation & audits. CERT-In
- Audit pack ready (policies, pentests, SBOMs, logs). CERT-In

12. References & useful CERT-In resources (important)

- CERT-In Directions under section 70B (28 Apr 2022) (full text & Annexures). CERT-In
- FAQs on Cyber Security Directions (clarifications on 6-hour reporting). CERT-In
- CERT-In Technical Guidelines on SBOM/QBOM/CBOM/AIBOM/HBOM (Oct 2024). CERT-In
- CERT-In Comprehensive Cyber Security Audit Policy Guidelines (Jul 25, 2025). CERT-In
- CERT-In reporting page & incident format (CERT-In website). CERT-In+1

Final notes (legal & practical)

- CERT-In rules have **regulatory force** and non-compliance can lead to directions/penalties; treat them as mandatory operational constraints for India operations or Indian customers. CERT-In
- Many requirements are **procedural and operational** (POC, 24×7 readiness, log retention) and require organizational/process changes as much as technical controls. Plan people/process changes with equal priority to engineering changes.