AWS INCIDENT RESPONSE

Meeting CERT-In's 6-Hour Incident Reporting Rule on AWS

India's CERT-In Cyber Security Directions give you six hours from noticing a cyber incident to filing an initial report. This is the practical playbook for AWS workloads in ap-south-1 and ap-south-2.

INDIA

By Matt Gurr

12 May 2026

ghostvector.ai/guides

Meeting CERT-In's 6-Hour Incident Reporting Rule on AWS

TL;DR

India's CERT-In requires you to file an initial incident report **within six hours of noticing** any of 20 reportable cyber incident categories. The rule applies to anyone running services used in India — including AWS workloads in ap-south-1 (Mumbai) and ap-south-2 (Hyderabad), and including foreign-headquartered companies serving Indian customers. To meet the deadline you need three things in place before an incident occurs: a defined trigger for "noticing," a pre-staged report template aligned to CERT-In's Annexure II format, and a logging stack that already complies with the 180-day-in-India retention rule. This guide walks through how to build all three on AWS.

What is the CERT-In 6-hour reporting rule?

The Indian Computer Emergency Response Team (CERT-In) issued its Cyber Security Directions on **28 April 2022** under section 70B(6) of the Information Technology Act 2000. The directions took effect on **28 June 2022** and remain in force.

The headline obligation is simple in wording and difficult in practice: every service provider, intermediary, data centre, body corporate, and government organisation must report any incident listed in Annexure I to CERT-In **within six hours of noticing** the incident, or being brought to notice of it.

Three details determine how the rule actually applies to you:

1. **Scope is broad.** "Body corporate" picks up nearly every company. There is no SME carve-out and no critical-infrastructure-only restriction. If your workload serves users in India, you are in scope.
2. **The clock starts on noticing, not detecting.** A SOC alert is not noticing. An L1 analyst triaging the alert and confirming it as a real incident is noticing. The distinction matters because most six-hour failures happen in the gap between alert-fired and someone-decided-it-is-real.
3. **The report can be preliminary.** CERT-In explicitly allows follow-up reports as facts emerge. You are not required to know the full impact in six hours; you

are required to start the formal communication.

Which incidents must be reported?

CERT-In's Annexure I lists 20 reportable incident categories. They group naturally into six clusters that map cleanly onto AWS detection sources:

Cluster	Annexure I categories	Primary AWS detection sources
Intrusion	Targeted scanning, unauthorised access, defacement, malicious code, attacks on servers and network appliances	GuardDuty, WAF logs, ALB/CloudFront logs, EC2/host EDR
Identity	Identity theft, spoofing, phishing, unauthorised access to social media accounts	GuardDuty IAM findings, CloudTrail, IAM Access Analyzer
Availability	DDoS attacks	Shield Advanced, CloudFront, WAF rate-based rules
Critical / OT	Attacks on critical infrastructure, SCADA, OT, IoT devices	AWS IoT Device Defender, custom detections
Data	Data breach, data leak	Macie, GuardDuty S3 findings, CloudTrail S3 data events
Emerging tech and services	Cloud system attacks, AI/ML system attacks, digital payments, mobile apps, fake apps, big data, blockchain, public Wi-Fi, e-Government	Security Hub aggregating findings across services

The cluster framing matters because your six-hour clock often starts before you know the technical category — what you do know is that *something is happening in the cloud cluster* or *something is happening in the data cluster*. Map your runbooks accordingly.

The 6-hour runbook for AWS workloads

A workable timeline from a confirmed incident to a submitted CERT-In report looks like this:

Minute 0 — Notice. An L1 or L2 analyst confirms an alert is a real incident in one of the 20 reportable categories. Record the exact timestamp in the incident ticket. *This is your t=0.*

Minutes 0-15 — Triage and classify. Determine the cluster (intrusion, identity, availability, critical, data, emerging tech). Identify the AWS account(s), region(s), and service(s) involved. Page the incident commander.

Minutes 15-30 — Preserve evidence. Run pre-staged containment automations. For an EC2 compromise that typically means: snapshot the EBS volumes, copy memory if EDR supports it, isolate via security group swap, copy the last 24 hours of CloudTrail and VPC flow logs to a forensics S3 bucket in the same region. Do not terminate instances until evidence is captured.

Minutes 30-45 — Gather reportable facts. Pull the data CERT-In needs: time of incident, time of detection, time of noticing, affected systems, IP addresses (internal and external), suspected vector, current containment status, contact person.

Minutes 45-90 — Draft and review. Populate the Annexure II template. Have the incident commander and a legal or compliance reviewer sign off. Loop in the responsible "Point of Contact" your organisation has registered with CERT-In (the directions require this designation in advance).

Minutes 90-120 — Submit. Email the report to incident@cert-in.org.in and also submit via the **incident.cert-in.org.in** portal. Keep proof of submission (email timestamps, portal acknowledgement).

You now have four hours of headroom. Use it to continue eradication and to draft your second update.

Pre-incident hardening — what to set up now

Six-hour compliance is mostly won before an incident, not during one. There are four AWS-specific items that organisations consistently underinvest in.

1. Logs maintained within India for 180 days

CERT-In requires ICT system logs to be retained within India on a rolling 180-day basis. On AWS that means:

- **CloudTrail** organisation trail with the S3 destination bucket in ap-south-1 or ap-south-2. Bucket-level Object Lock with a 180-day retention period is the cleanest way to guarantee compliance.
- **CloudWatch Logs** retention set to ≥180 days for all log groups holding security-relevant data.
- **VPC Flow Logs** delivered to S3 in an Indian region.
- **Application logs** (ALB access logs, CloudFront real-time logs, RDS audit logs) either stored in an Indian region or shipped to a central S3 bucket in ap-south-1.
- **Cross-region replication** to a non-Indian region for resilience is fine — but the Indian copy must always be the system of record.

A common mistake is to use ap-south-1 as the workload region but ship logs to a central observability account in us-east-1. Under the directions, that breaks compliance even though no Indian data has crossed the border, because the *log evidence* you would rely on during an investigation is sitting outside India.

2. Clock synchronisation to NPL or NIC

The directions require ICT system clocks to be synchronised with the NTP servers of the National Physical Laboratory (NPL, time.nplindia.org) or the National Informatics Centre (NIC, samay1.nic.in / samay2.nic.in) — or servers traceable to them.

Amazon Time Sync Service (the link-local 169.254.169.123 service available on EC2) is traceable to UTC via a fleet of redundant GPS antennas and atomic reference clocks, but it is not explicitly traceable to NPL or NIC. There is no published statement from AWS that resolves the ambiguity.

The conservative configuration on EC2 instances running in scope is to override the default chrony or ntpd configuration to use:

```
server time.nplindia.org iburst
server samay1.nic.in iburst
server samay2.nic.in iburst
```

Or to use Amazon Time Sync as a primary with NPL/NIC as secondary sources, depending on your network reliability constraints. Document the decision and the rationale either way — auditors will ask.

3. A registered CERT-In Point of Contact

The directions require every in-scope organisation to designate a "Point of Contact" (PoC) responsible for interfacing with CERT-In, and to keep CERT-In informed of the PoC details. Do not discover during an incident that your PoC has changed jobs.

4. Pre-staged Annexure II templates

CERT-In specifies a reporting format in Annexure II. Have the template loaded into your IR platform (Jira Service Management, ServiceNow, PagerDuty, or whichever you use) as a form, with fields that mirror Annexure II exactly. The six-hour clock is too tight to be assembling a report from a Word template under pressure.

AWS region selection and data residency interaction

India operates two AWS regions: **ap-south-1 (Mumbai)** and **ap-south-2 (Hyderabad)**. Either satisfies the in-India log retention requirement. There are three implications for incident response:

1. **Cross-region log replication within India is permitted and recommended.** Replicating CloudTrail and VPC flow logs from ap-south-1 to ap-south-2 (or vice versa) gives you regional resilience without breaching residency.
2. **SES is not available in ap-south-1 or ap-south-2 at time of writing.** If your incident notification workflow depends on SES, you are sending from outside India — which is fine for outbound notifications but worth noting in your runbook.
3. **Bedrock and some newer services have variable Indian regional availability.** If you are responding to an "attacks on AI/ML systems" incident under Annexure I and the model is hosted outside India, the incident is still in scope because the affected service is consumed by Indian users.

Common mistakes

Five patterns we see repeatedly when reviewing CERT-In readiness for AWS workloads:

- **Treating "noticing" as "investigating."** Some organisations interpret noticing as the point at which they fully understand the incident. The directions do not support that reading. Notice triggers when a responsible person becomes aware.
- **Centralising logs in a non-Indian region for convenience.** A globally consistent observability stack often violates the 180-day-in-India rule. Build a regional split.
- **Relying on Amazon Time Sync without documentation.** Either configure NPL/NIC explicitly, or write down the rationale for relying on Amazon Time Sync's UTC traceability — but do not ignore the question.
- **No pre-registered PoC.** Discovering during an incident that nobody is authorised to file the report adds hours you do not have.
- **Treating the six-hour report as the final report.** It is not. Plan for follow-up reports at 24 hours, 72 hours, and at incident closure.

What to do this week

If you operate AWS workloads serving Indian users and you have not already done a CERT-In readiness assessment, three concrete actions return the most value in the first week:

1. **Audit your log destinations.** Confirm every security-relevant log is stored in ap-south-1 or ap-south-2 with ≥180-day retention.
2. **Register or refresh your CERT-In Point of Contact.** Send an updated PoC notification to CERT-In if details have changed.
3. **Run a six-hour tabletop.** Use a realistic scenario (compromised IAM access key, S3 exfiltration, or a GuardDuty critical finding on EC2). Time yourselves from "notice" to "submitted report." Find out where the friction is *before* it is a real incident.

The 6-hour rule is unforgiving, but the system underneath it is mostly mechanical. Organisations that get caught out almost always knew the rule existed — what they lacked was the muscle memory to execute under time pressure.

Related guides

- AWS Incident Response in APAC — Pillar guide — the regulatory and technical overview across Australia, Singapore, India, and ASEAN.
- APRA CPS 234 notification obligations on AWS — the Australian FSI equivalent.

- MAS TRM and AWS incident response — the Singapore FSI equivalent with a 1-hour clock.
- Ghost Vector managed detection — our managed detection service includes CERT-In-aligned reporting workflows.