MatrixGard

INCIDENT RESPONSE, 2026 EDITION

Incident Response Sheet: The First 60 Minutes

A leadership sheet for faster decisions and a cleaner root-cause review. Use it two ways: score your team today, before anything breaks, and keep it open during a real incident. Structured on NIST SP 800-61 Rev. 3 (April 2025), with the India reporting clocks in a box after stage 4.

25 questions | 5 stages of 5 | Max score 50 | Last reviewed: November 2026

How to score

Yes = 2 | Partly = 1 | No = 0

Yes: we always do this. Partly: we sometimes miss it. No: we usually skip it.

Score each line on what happened in your last real incident or drill, not on what the plan says.

The arithmetic

25 questions x 2 points = **50 points**.

5 stages x 10 points = **50 points**.

Each stage is tagged with the NIST CSF 2.0 categories that 800-61r3 uses.

STAGE 1 · BEFORE THE INCIDENT · GOVERN, IDENTIFY, PROTECT

Ready before it starts

Leadership question: "If this happened tonight, who would do what?"

Score ____ / 10

	QUESTION	YES	PARTLY	NO
1.1	A written response plan names the roles: incident owner, communications lead and scribe.	2	1	0
1.2	Severity levels are defined by customer, data and revenue impact, so nobody debates them mid-incident.	2	1	0
1.3	A contact list is ready: on-call, cloud provider support, legal, and the CERT-In reporting route.	2	1	0
1.4	Cloud, identity and application logs are on, collected in one place, and kept long enough. CERT-In: a rolling 180 days, kept within India.[2]	2	1	0
1.5	We have rehearsed an incident (a tabletop exercise or a drill) in the last 12 months.	2	1	0

STAGE 2 · MINUTES 0 TO 15 · DE.AE, RS.MA, RS.MI

Declare and contain

Leadership question: "Who owns this incident right now?"

Score ____ / 10

	QUESTION	YES	PARTLY	NO
2.1	One incident owner (not necessarily the most senior person) is named and confirms the role.	2	1	0
2.2	A dedicated channel and a timestamped timeline document start straight away.	2	1	0
2.3	Risky changes and deployments are frozen.	2	1	0
2.4	Severity is set, and if personal data or a reportable cyber incident may be involved, the time we noticed it is written down: the reporting clocks start there.	2	1	0
2.5	The fastest safe containment is done: roll back the last risky change, fail over, or revoke exposed keys and sessions.	2	1	0

STAGE 3 · MINUTES 15 TO 30 · RS.AN

Collect the evidence

Leadership question: "What changed right before the impact started?"

Score _____ / 10

	QUESTION	YES	PARTLY	NO
3.1	Logs, metrics and traces are preserved before they rotate, and affected systems are snapshotted before anyone rebuilds them.	2	1	0
3.2	Recent deployments, configuration changes and access changes are listed.	2	1	0
3.3	Error spikes are checked against dependencies and sign-in anomalies (unusual logins, new keys, new admins).	2	1	0
3.4	Every action is recorded with the time and the person who did it.	2	1	0
3.5	The team stays on evidence, not on early theories or blame.	2	1	0

STAGE 4 · MINUTES 30 TO 60 · RS.MI, RS.CO

Narrow the blast radius and communicate

Leadership question: "What is affected, what is not, and when is the next update?"

Score _____ / 10

	QUESTION	YES	PARTLY	NO
4.1	The faulty component, region or account is isolated, and risky third-party integrations are paused.	2	1	0
4.2	There is a clear list of which customers, data and regions are affected and which are safe.	2	1	0
4.3	Critical paths (sign-in, payments) are protected first.	2	1	0
4.4	Internal updates go out on a fixed cadence (for example every 30 minutes), and a plain, honest customer update has a time.	2	1	0
4.5	Someone owns the regulator clock: the CERT-In report within 6 hours where the Directions apply, and the Data Protection Board notice once DPDP Rule 7 is in force (see the India box).	2	1	0

India: the reporting clocks (reference, not scored)

- **CERT-In, 6 hours.** Service providers, intermediaries, data centres, body corporates and government organisations must report the cyber incidents listed in Annexure I to CERT-In within 6 hours of noticing them or being told about them (incident@cert-in.org.in).[2]
- **CERT-In, 180 days of logs.** The same entities must keep logs of all their ICT systems for a rolling 180 days, within Indian jurisdiction, and hand them to CERT-In with an incident report or on request.[2]
- **DPDP Rules 2025, Rule 7 (personal data breach).** Tell each affected person without delay, in plain language: what happened, the likely consequences, what you are doing and what they can do. Tell the Data Protection Board without delay, then send the detailed report within 72 hours of becoming aware (or a longer period the Board allows in writing).[3]
- **When Rule 7 applies.** The Rules were published in the Gazette on 13 November 2025 (G.S.R. 846(E)). Rule 1(4) brings Rule 7 into force eighteen months after publication, which is 13 May 2027. Rehearse it now.[3]

STAGE 5 · AFTER THE FIRST HOUR · RC.RP, RC.CO, ID.IM

Recover and improve

Leadership question: "How do we make sure this does not happen again?"

Score _____ / 10

	QUESTION	YES	PARTLY	NO
5.1	Systems are restored from a known-good state and checked before they take traffic again.	2	1	0
5.2	Recovery status is shared with customers and internal teams until the incident is closed.	2	1	0
5.3	A post-incident review has a named owner and is blameless.	2	1	0
5.4	The top actions are tracked to closure, each with an owner and a date.	2	1	0
5.5	The plan, playbooks and this sheet are updated with what we learned.	2	1	0

YOUR RESULT

Add it up

1. Ready before it starts _____ / 10
2. Declare and contain _____ / 10
3. Collect the evidence _____ / 10
4. Narrow the blast radius and communicate _____ / 10
5. Recover and improve _____ / 10

Total _____ / 50

0 to 24

Set up the basics

Name the incident owner role, define severity, and switch on central logging. Those three make every later step faster.

25 to 39

Developing control

Containment works; evidence and communication slip. Write a one-page playbook and run a drill against it.

40 to 50

Strong response

Automate evidence capture and keep rehearsing, including the India reporting clocks.

The bands are our rule of thumb for where to start, not an industry benchmark.

Want us to go through it with you?
Free 20-minute review of how your team would handle the first hour.
matrixgard.com/review/

SOURCES (CHECKED NOVEMBER 2026)

1. NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (final, April 2025). csrc.nist.gov/pubs/sp/800/61/r3/final
2. CERT-In Directions under section 70B(6) of the IT Act, 28 April 2022, paragraphs (ii) and (iv). cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
3. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India Extraordinary No. 760, 13 November 2025, Rules 1 and 7. egazette.gov.in/WriteReadData/2025/267650.pdf