

Major Incident Checklist

One page for the first hour of a major incident. Print it or pin it in your incident channel. From the ITOC360 guide to major incident management.

1. Declare a major incident if ANY one is true

- ☐ A customer-facing critical service is down or unusable for all or most customers.
- ☐ Payments, logins, orders or another revenue path fail above the agreed threshold (e.g. 5% of requests).
- ☐ Data loss, data corruption or a suspected security breach is possible.
- ☐ An SLA or regulatory reporting deadline is at risk.
- ☐ More than one team is needed to restore service.
- ☐ Impact is uncertain but potentially severe, and growing.

When in doubt, declare. Anyone can declare; the major incident manager can downgrade later.

2. The first 15 minutes

Minute	Step	Done
0	Declare: open one incident record, one channel and a bridge call	
by 5	Mobilize: page the major incident manager, technical lead and communications lead	
by 10	Assess: what customers see, how many, since when, getting worse?	
by 15	Communicate: first internal and external update, with the next update time	

3. Roles

Role	Owns	Does not
Major incident manager	Priorities, roles, cadence, escalation, declaring resolution	Debug
Technical lead	Diagnosis and the restoration plan	Write customer updates
Communications lead	Every update, on schedule	Join the technical debate
Scribe	The timeline: what was seen, decided and done, with times	Make decisions

Hand over any role after 4 to 6 hours, with a verbal summary and a note in the timeline.

4. Update cadence

Audience	Channel	SEV1	SEV2
Responders	Incident channel + bridge	Continuous	Continuous
Leadership	Email or leadership channel	Every 30 min	Every 60 min
Customers	Status page, in-app banner	Every 30 min	Every 60 min
Support team	Support channel, pinned summary	Every 30 min	Every 60 min

Every update says: what is affected (in customer language) · what we know and are doing · any workaround · when the next update comes. Promise the next update time, never a fix time.

5. Close out

- ☐ Restore service first (rollback, failover, feature flag, traffic shift); fix the cause later.
- ☐ Declare resolved when business impact has ended, and send a final update.
- ☐ Schedule a blameless post-incident review within 5 business days, using the timeline.
- ☐ Open a problem record with an owner, so the root cause is fixed permanently.