

Post-Incident Review: Filled Example

FICTIONAL EXAMPLE: the organization, systems, people, times and figures in this document are invented.

1. Incident summary

Field	Value
Incident ID	EXAMPLE-2041
Service(s) affected	Customer sign-in (fictional company: Larkfield Outdoor Supply)
Severity / priority	P1, as recorded by the team
Impact started	2026-03-11 09:58 UTC
Detected	2026-03-11 10:03 UTC (automated alert)
Service recovered	2026-03-11 10:31 UTC
Resolved	2026-03-11 11:40 UTC
Review facilitator (role)	Engineering manager, payments (not involved in the response)

2. Impact

About a third of sign-in attempts failed for 33 minutes. Customers who were already signed in were not affected. No data was lost or exposed. Roughly 140 support contacts mentioned sign-in during the window (from the support tool's tag report).

3. Timeline (key moments)

Time (UTC)	What happened	Source
09:55	Scheduled TLS certificate rotation runs on the edge load balancers.	Change log
09:58	Sign-in error rate begins to rise.	Metrics
10:03	Error-rate alert fires for the sign-in service.	Alerting
10:06	On-call engineer acknowledges and opens the incident channel.	Chat
10:11	Major incident declared; commander, technical lead and comms lead named.	Chat
10:15	First status page update published, next update promised at 10:35.	Status page
10:24	Previous certificate restored on the load balancers.	Change log
10:31	Sign-in success rate back to normal; test sign-ins confirmed.	Metrics, synthetic checks
11:40	Corrected certificate chain deployed; incident closed.	Change log

4. Contributing factors

- The new certificate was deployed without its intermediate certificate, so some clients could not validate it.
- The rotation script checked that the certificate file existed but did not validate the full chain.

- Older mobile app versions were most affected; staging tests used only current browsers.

Root cause: the team agreed that the missing intermediate certificate combined with the lack of chain validation. No other cause was identified.

5. What went well

- The alert fired within five minutes of impact.
- Rollback of the certificate took under ten minutes once decided.
- Status updates went out when promised.

6. Follow-up actions

#	Action	Owner	Due	Verification
1	Add full chain validation to the rotation script and fail on an incomplete chain	Platform team	2026-03-25	A test run with a deliberately incomplete chain fails
2	Add an older mobile client to the synthetic sign-in checks	Mobile team	2026-04-01	Synthetic check visible on the sign-in dashboard
3	Move certificate rotations out of peak sign-in hours	Release engineering	2026-03-18	Rotation schedule updated in the change calendar

7. Open questions

- Why did the staging environment accept the incomplete chain? Owner: platform team, by 2026-03-20.