

Sample After-Action Report

The report the Calmdrill Game Master wrote at the end of a drill of CD-01, The 02:14 Certificate.

Scenario	Source	Company
CD-01 The 02:14 Certificate	Internal scripted playtest, Claude Sonnet	Harbourline (fictional)

Pink: the evaluator's record. The report as the Game Master delivered it, for a person to review and sign. Our four players were scripted to make the classic mistakes. We changed the formatting and corrected the date line; everything else is as the AI wrote it.

Organisation	Harbourline (fictional)
Exercise type	Discussion-based tabletop exercise (AI-facilitated)
Scenario	CD-01 · The 02:14 Certificate · Reliability
Mode	Team
Date and duration	30 September 2026 · 65 minutes (simulated: T+01:15)
Setting	Harbourline (fictional)
Programme / framework context	Annual incident response test; SOC 2
Facilitator	Calmdrill Game Master (AI) · Human lead: Sam (Incident Commander, Engineering Manager)
Report status	Draft for human review

1. Participants

Name / initials	Exercise role	Usual job role
Sam	Incident Commander	Engineering Manager
Ana	Tech Lead (held the pager)	Backend developer
Jo	Comms Lead	Head of Customer Success
Raj	Scribe	Platform engineer

Roles played by the facilitator: CEO (Dana), CTO (Marcus), Security Lead (Ines), Head of Support (Priya), secondary on-call SRE (Leo), Head of Platform (Tom, auto-reply only), Enterprise customer (Brightwater Dental).

2. Objectives

1. Recognise and declare a partial, growing outage quickly.
2. Separate a tempting red herring (a recent deploy) from the evidence.
3. Find a certificate chain failure in an estate that "auto-renews everything".
4. Handle a break-glass access problem when the one person who knows is unavailable.
5. Keep customers and Enterprise accounts informed while impact grows.

3. Scenario summary

As presented to players: At 02:19 UTC on a Tuesday, the on-call engineer is paged because the `auth-svc` login success rate has fallen to 71%, having been 99.6% all evening. Most of the company is asleep. Impact grows over the following hour, and an Enterprise customer, support, the CTO and the CEO all need attention.

What was really happening (revealed at debrief): The internal intermediate certificate authority, created by hand three years earlier with a 3-year validity, expired at 02:14:07 UTC. `cert-manager` renews only leaf certificates and nobody monitored the intermediate, so every certificate showed READY. Existing connections kept working and only new connections failed, so new logins broke first and the damage spread. A 01:52 `web-app` deploy was an unrelated red herring. The fix was a new intermediate issued from the root key, held behind two-of-three break-glass approval, followed by re-issuing leaf certificates and rolling restarts.

4. Timeline

Sim time	Event / decision	Who
T+00:00	Page fires: login success rate 71%	GM inject
T+00:02	Ana acks, checks Datadog and Argo CD, finds the 01:52 <code>web-app</code> deploy and starts a rollback	Ana
T+00:08	Second page: login success rate below 60%	GM inject
T+00:10	<code>web-app</code> rollback completes with no effect. Customer tweet appears.	Ana / GM
T+00:12	Ana pages Sam. Sam declares SEV1 and opens #inc-0214.	Ana, Sam
T+00:12	Raj suggests, and Sam approves, a restart of all <code>auth-svc</code> and <code>billing-svc</code> pods. Login success falls from 41.5% (T+00:15) to 24.6% (T+00:20) and later to about 5%.	Raj, Sam
T+00:15	Head of Support asks what to tell customers	GM inject
T+00:17	First status page update: "We are aware of an issue and are investigating."	Jo
T+00:20	<code>kubectl get certificates -A</code> shows every certificate READY	Ana
T+00:22	Second status page update: "Some customers can't log in. If you're already logged in you can keep working." Next update 03:10.	Jo
T+00:23	Leo paged and joins. Sam assigns him the <code>notify-svc</code> backlog at T+00:25.	Sam
T+00:25	<code>notify-svc</code> queue depth page. Hint 1 used.	GM / Ana
T+00:30	Ana runs <code>openssl s_client -showcerts</code> on <code>billing-svc</code> and sees the expired intermediate (verify code 10)	Ana

Sim time	Event / decision	Who
T+00:34	Cause identified. Third status page update: "Identified: an internal certificate expired". Next update 03:20.	Ana, Jo
T+00:35	Root key access denied (needs BreakGlassAdmin). Slack message to Tom returns an on-holiday auto-reply.	Ana, Sam
T+00:38	Sam finds the two-of-three break-glass approvers on the wiki	Sam
T+00:41–00:43	Sam phones Marcus (CTO) and Ines (Security Lead), who both approve in Okta	Sam
T+00:44	Jo emails Enterprise accounts proactively	Jo
T+00:45	Enterprise customer asks for an ETA on their 08:00 invoice run	GM inject
T+00:48	BreakGlassAdmin granted. The <code>ClusterIssuer</code> update and <code>cmctl</code> re-issue were already prepared.	Ana
T+00:50	Ledger consumer-lag page. Sam tells Marcus to keep off the cluster and gives him CEO and Enterprise escalations. Ana issues the new intermediate.	GM, Sam, Ana
T+00:52	Jo tells the Enterprise customer a fix is rolling out and that the 08:00 run will be confirmed by 04:00	Jo
T+00:55–01:05	<code>cmctl renew --all -A</code> re-issues 62 of 62 certificates	Ana
T+01:00	CEO asks for a board summary and about service credits	GM inject
T+01:05–01:15	Rolling restart: wave 1 complete, wave 2 in progress. Login success 74.6% at T+01:15. No duplicates found so far.	Ana, Leo
T+01:15	The status page had passed its own 03:20 "next update" promise. Jo posts "Monitoring" (next update 04:00) and proposes proactive Enterprise credits. Drill ended.	Jo, Sam

Key moments: detection T+00:00 → declared T+00:12 · first external comms T+00:17 · mitigation started T+00:50 · resolution not reached (logins 74.6% at T+01:15; queue drain and reconciliation still pending).

5. Results against the rubric

Dimension	Score (1–4)	Evidence
Detection & triage	3	Ana acked and checked Datadog at once, and SEV1 was declared at T+00:12, slightly after the second page (T+00:08). Scope (only new logins failing) was clear by T+00:22.
Coordination & roles	3	Clear IC. Leo was given the <code>notify-svc</code> backlog (T+00:25) and Marcus was kept off the cluster (T+00:50). Ana worked alone until T+00:12, and the T+00:12 restart was approved without challenge.
Communication	3	Status updates at T+00:17, T+00:22 and T+00:34, and a proactive Enterprise email at T+00:44. The first update was vague, and the page later passed its own 03:20 promise.
Technical response	2	The <code>web-app</code> rollback (T+00:02 to T+00:10) and the pod restart (T+00:12) were made without verification, and the restart worsened impact (41.5% to about 5%). The chain was inspected at T+00:30 and each restart wave was verified.
Decisions under uncertainty	2	The restart was approved without stated reasoning or trade-offs. Break-glass access was well handled, but disabling mTLS verification was never weighed as an option.
Recovery & obligations	2	Duplicate checks, an Enterprise 08:00 commitment and a proactive credit proposal were in place, but the drill ended before verification (logins 74.6%, queues still draining).

6. What went well

- **Evidence-led diagnosis after the hint.** Ana inspected the full chain at T+00:30 and had the expired intermediate identified by T+00:34.
- **Fix prepared in parallel.** The `ClusterIssuer` update and `cmctl` re-issue were ready before access arrived, and each restart wave was verified.
- **Command and delegation.** Sam phoned the approvers directly (T+00:41 to T+00:43), gave Leo the `notify-svc` backlog (T+00:25) and kept Marcus off the cluster while giving him CEO and Enterprise work (T+00:50).
- **Honest, proactive communication.** The T+00:22 update told customers logged-in users could keep working, Jo emailed Enterprise accounts at T+00:44 before being asked, and Jo gave the CTO a clear SLA and credits position.
- **Candid reflection.** The team named its own restart mistake and the "reacted before we'd looked" lesson.

7. What to improve

- **Rollback before evidence (T+00:02 to T+00:10).** The deploy was CSS-only, and nobody checked whether the errors were TLS-related. Eight minutes were spent, and nobody else was woken until the second page had fired.
- **Restart approved without evidence (T+00:12).** Login success fell from 41.5% to about 5%. No one asked what evidence supported it, and the effect of dropping pooled connections was not considered.
- **First status update was vague (T+00:17).** It gave no impact or workaround. The T+00:22 update corrected this.
- **Status page cadence.** At T+01:15 the page still said "next update 03:20" and was past that time.
- **Break-glass single point of failure.** Tom, the third approver, was unreachable, and there was no fallback approver or phone list.
- **Emergency options not weighed.** Disabling mTLS verification was never considered, so no owner or exception process was tested.

8. Improvement actions

#	Action	Owner	Due	Success measure	Status
1	Alert on expiry of every certificate in the chain, including root and intermediate CA, at 30 and 7 days, paging on-call rather than only Slack	Platform	16 Oct 2026	A test alert on a dummy CA fires and pages within an hour	Open
2	Break-glass contact tree: a fourth named approver, phone numbers for all approvers and a 2 a.m. call order	Security	13 Oct 2026	A timed out-of-hours dry run gets two approvals within 15 minutes	Open
3	IC checklist: "errors first, then changes. No rollback or restart without one line of evidence and a named approver"	IC rotation (Sam)	9 Oct 2026	Appears in the next drill's log and the wiki links to it	Open
4	Status page templates for partial login outages, with "what's affected" and "what you can do" wording and a 30-minute update reminder	Jo	16 Oct 2026	In the next drill, the first update includes impact and workaround within 15 minutes	Open

#	Action	Owner	Due	Success measure	Status
5	Certificate and expiry inventory: intermediate CA, Apple push certificate, Okta SAML certificate, domain renewals, each with owner and expiry date	Platform with Security	23 Oct 2026	Every item has a named owner and alerts to more than one person	Open
6	Automate intermediate CA rotation and write a re-issue runbook	Platform	6 Nov 2026	Rotation tested in staging and the runbook reviewed by a second engineer	Open
7	Emergency mTLS-off exception procedure: IC and Security agree, time-boxed, logged with a revert owner	Security with IC	30 Oct 2026	Procedure documented and rehearsed in the next drill	Open

9. Plan and documentation updates

- Add the "evidence before rollback/restart" checklist to the incident template (action 3).
- Publish a break-glass runbook with a fourth named approver, phone numbers and a 2 a.m. call order (action 2).
- Add status page templates and a 30-minute update reminder to the communications runbook (action 4).
- Add a service-credit decision guide for Enterprise SLAs. Owner: Marcus. Due: 23 Oct 2026.
- Book the post-incident review within five working days, as the incident process requires (by 7 Oct 2026). Owner: Sam.
- Record the emergency mTLS-off exception procedure in the security policy (action 7).

10. Evidence summary

This exercise tested availability incident response and recovery procedures, including a scenario in which a key person was unavailable. It is intended to support evidence for SOC 2 Trust Services Criteria CC7.4 and CC7.5 and, where Availability is in scope, A1.3 (testing of recovery plan procedures). It also tests the documented incident process: declaration, roles, status-page cadence and post-incident review. Whether it satisfies a specific requirement is a matter for the organisation and its auditor.

Evidence attached / retained:

- ☐ This report (signed)
- ☐ Attendance record
- ☐ Exercise log / transcript
- ☐ Improvement actions entered in the tracker
- ☐ Updated plan or runbooks (if any)

11. Sign-off

Report prepared with the Calmdrill Game Master (AI-facilitated). Reviewed and approved by: _____ Role: _____
 Date: _____