# Phase 4 Facilitator Guide – Technical / Cyber Team

## Phase Overview: Resolution and Accountability (T+90 to T+120)

In the final phase, the Technical team must deliver closure: forensic evidence, summary of system impacts, and input into breach documentation. Clarity and accuracy are essential as this forms the foundation for legal and ministerial reporting.

This phase tests:

* Evidence collation and incident mapping
* Input into breach and regulatory documentation
* Transition to recovery posture

## Injects Relevant to Technical

### P4-1 (T+90 to T+100)

**INJ016:** Audit VM access granted – logs available for review

**Facilitator Notes (P4-1)**

* Tech must examine logs for attacker behaviour and dwell time
* Should report findings to Coordinator and Legal
* Prompt:
  + "Have you reviewed the audit logs for indicators of compromise?"
  + "What anomalies or patterns are now confirmed?"

### P4-2 (T+100 to T+110)

**INJ017:** Suspicious cron job found in compromised environment  
**INJ019:** Crane override failure – triggered again by same cron

**Facilitator Notes (P4-2)**

* Tech should correlate evidence from log analysis and system events
* Link incident cause with operational failures for the report
* Prompt:
  + "Is this the same exploit or a variant?"
  + "What is your recommendation for immediate system recovery?"

### P4-3 (T+110 to T+120)

**INJ020:** Prepare timeline of attack vector and escalation chain  
**INJ021:** Summary report must include system impact, logs, and fixes

**Facilitator Notes (P4-3)**

* This is the closeout summary from Technical
* It will inform the Legal and Executive narratives
* Prompt:
  + "Is your timeline aligned with Coordinator and Ops logs?"
  + "Are you handing over a consolidated report with remediation notes?"

## Technical Role Expectations

* Finalise forensic and attack chain analysis
* Document and submit system impact report
* Coordinate with Legal and Coordinator on summary package

**Key Policy References:**

* Technical Forensics SOP – §7.2
* Incident Recovery Protocol
* Breach Evidence Handling Checklist

## Technical Decision Point – Phase 4

**Decision: Finalise and Submit Technical Impact Report?**

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Description** | **Implication** | **Score** |
| ✅ Submit full logs, exploit chain, and fixes | Precise | Enables confident reporting and follow-up | +10 |
| ⚠️ Submit partial info, defer full for post-review | Conservative | Some delay, still useful | +1 |
| ❌ Delay or submit nothing clear | Major flaw | Weakens entire incident narrative | -9 |

## End-of-Phase Checkpoint Prompt

At or near **T+120**, facilitator should ask:

"Technical team — has your full impact report been delivered? Are all logs and exploit paths documented and shared with Legal and the Coordinator?"

## Tip for Facilitator

If Tech is behind:

* Reference INJ017–INJ021
* Ask for status of the audit log review (INJ016)
* Confirm submission format and who receives it

#### End of Phase 4 – Technical / Cyber Team Facilitator Guide