# Phase 2 Facilitator Guide – Incident Coordinator Team

## Phase Overview: Public & Internal Chaos (T+30 to T+60)

Phase 2 is a critical tracking window for the Incident Coordinator. With injects affecting multiple roles, the Coordinator must ensure injects are logged, responses documented, and decision points tracked. The incident is likely now public-facing or nearing that threshold.

This phase tests:

* Cross-role observation and timeline discipline
* Documentation of escalation decisions
* Recording of technical findings and legal responses

## Injects Observed by Coordinator

### P2-1 (T+30 to T+40)

**INJ004A:** SSH log anomalies (Tech)  
**INJ004B:** Vendor unable to connect (Ops/Tech)  
**INJ004C:** Vendor payment flag (Exec/Legal)

**Facilitator Notes (P2-1)**

* Coordinator should begin timeline for all three parallel issues.
* Encourage tagging roles, symptoms, and escalation.
* Prompt:
  + "Are you tracking which teams are taking action on each issue?"
  + "Have you started tagging responses and policy references?"

### P2-2 (T+40 to T+50)

**INJ005A:** Vendor session ends abnormally (Tech/Ops)  
**INJ005C:** Insurer contacts Legal about clause 4.7

**Facilitator Notes (P2-2)**

* Expect cross-talk between Legal and Exec, and Tech escalation.
* Coordinator should tag policy references and note decision time.
* Prompt:
  + "Has any team declared this an incident?"
  + "Which injects link to escalation discussions?"

### P2-3 (T+50 to T+60)

**INJ006A:** Cron job suppresses alert (Tech)  
**INJ006B:** Journalist contacts CEO  
**INJ006C:** Media interview pressure confirmed  
**INJ006D:** Physical access failure (Ops)

**Facilitator Notes (P2-3)**

* This is a dense window. Coordinator should highlight cross-role intersections.
* Ensure any declared public escalation is timestamped and noted.
* Prompt:
  + "Have you documented the trigger for the CEO media response?"
  + "Is the system compromise (cron) now formally part of the incident record?"

## Coordinator Role Expectations

* Maintain accurate timeline
* Document cross-team triggers and handoffs
* Tag escalation points and decisions
* Align team actions to scenario progression

**Key Policy References:**

* Coordinator Handbook – Page 2
* Incident Log Template

## Coordinator Decision Point – Phase 2

**Decision: Formalise Public-Facing Crisis in Log?**

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Description** | **Implication** | **Score** |
| ✅ Timestamp and tag public escalation in log | Clear traceability | Enables debrief, protects audit chain | +9 |
| ⚠️ Record team activity only, no escalation tag | Partial view | Gaps in accountability trail | +1 |
| ❌ Log remains internal only | Poor practice | Major omissions, review failure | -6 |

## End-of-Phase Checkpoint Prompt

At or near **T+60**, facilitator should ask:

"Coordinator — what timeline entries exist for escalation, media contact, and system compromise? Have you tagged all major injects and noted policy intersections?"

Ensure incident log includes both team responses and external triggers.

## Tip for Facilitator

If logging is light:

* Prompt review of INJ006A–D
* Encourage back-tagging of Phase 2 decisions
* Validate use of Incident Log Template and team references

#### End of Phase 2 – Incident Coordinator Facilitator Guide