**Phase 4: Resolution and Accountability (T+90 to T+120)**

**Overview**

Phase 4 transitions participants from crisis response into formal closure and accountability. Teams must now consolidate their decisions, finalise communications, submit reports, and ensure that the incident is properly documented for internal and external audiences.

Stakeholder expectations are high. Executives must deliver a formal briefing. Legal must lock in the breach notification. Technical teams must submit forensics. The Media team prepares the final message. Operations closes out physical site activities. The Incident Coordinator brings the entire story together into a log that underpins the debrief and performance scoring.

Facilitators should emphasise discipline, closure, and clarity. Delayed decisions here still impact the perceived success of the response.

**Injects**

**P4-1: T+90 to T+100**

* **INJ013A:** Access granted to audit VM and forensic logs. *(Resource: VM-Audit, Technical)*
* **INJ013K:** Email – CFO: “Before approving any brief, can we confirm if insurer cover still applies?” *(Resource: VM-Email, Executive, Legal)*
* **INJ013L:** Email – Comms Team: “We need a photo of the CEO at the terminal — can you arrange it?” *(Resource: VM-Email, Media, Executive)*
* **INJ013M (Noise):** Email – Staff Suggestion Box: “Can we get more vegetarian lunch options?” *(Resource: VM-Email, All Roles)*

**P4-2: T+100 to T+110**

* **INJ013B:** Reported crane override failure disrupts container drop. *(Resource: VM-Logs, Ops)*
* **INJ013C:** Suspicious cron job detected by audit team on scheduler. *(Resource: VM-Email, Technical)*
* **INJ013N:** Email – Dock Supervisor: “Crane team confused — no clarity if system is safe or overridden.” *(Resource: VM-Email, Ops, Technical)*
* **INJ013O:** Email – Legal Intern: “Does the cron job count as ‘persistence’ under the cybersecurity act?” *(Resource: VM-Email, Legal)*
* **INJ013P (Noise):** Email – HR Reminder: “Don’t forget to nominate your peers for the Excellence Awards!” *(Resource: VM-Email, All Roles)*

**P4-3: T+110 to T+120**

* **INJ013D:** Terminal room access attempt logged — badge not authorised. *(Resource: VM-Security Logs, Ops, Tech)*
* **INJ013E:** Breach notification draft submitted for approval. *(Resource: VM-Email, Legal, Executive)*
* **INJ013F:** Legal team shares case precedent relevant to breach. *(Resource: VM-Email, Legal)*
* **INJ013G:** External tweet claims containers misrouted again. *(Resource: VM-Social, Media, Executive)*
* **INJ013H:** Journalist requests CEO comment for closing story — deadline in 30 minutes. *(Resource: VM-Email, Media, Executive)*
* **INJ013I:** Reminder to tag all deviations and prepare logs for scoring. *(Resource: VM-Email, Incident Coordinator)*
* **INJ013J:** Request for end-of-day briefing log from Incident Coordinator. *(Resource: VM-Email, Exec, Incident Coordinator)*
* **INJ013Q:** Email – Angela Poole (External Affairs): “I strongly recommend we delay media statement until CEO is fully briefed.” *(Resource: VM-Email, Media, Executive)*
* **INJ013R:** Email – Policy Advisor: “Legal precedent shared may not apply to digital breaches — should we be citing it?” *(Resource: VM-Email, Legal)*
* **INJ013S (Noise):** Email – Port Rec Club: “BBQ moved to Friday due to weather.” *(Resource: VM-Email, All Roles)*
* **INJ013T:** Email – Department of Infrastructure: “Please submit full incident report and decision record for ministerial review.” *(Resource: VM-Email, Executive, Incident Coordinator, Legal)*

**Team Expectations and Decisions – Phase 4**

**Executive**

**Expectations:**  
• Finalise all external-facing messaging and confirm internal alignment.  
• Provide a complete end-of-incident status briefing for stakeholders.  
• Respond to media and ministerial inquiries with a unified stance.

**How they make decisions:**  
• INJ013H (journalist comment request) and INJ013T (ministerial report request) require coordinated public leadership.  
• CFO concern in INJ013K may delay sign-off unless clarified with Legal.  
• Use: *Executive Wrap-Up Checklist*, *CEO Comms Briefing Template*, and *Policy Binder*.

**Key Decision: Finalise Executive Status Brief for All Stakeholders?**  
• **Trigger:** INJ013T (Govt request), INJ013H (media deadline), and INJ013E (legal breach draft)  
• **Policy:** *Exec Crisis Wrap Guide, Section 3*

| **OptionDescriptionImplicationScore** |  |  |  |
| --- | --- | --- | --- |
| ✅ | Publish cohesive, signed briefing | Strong leadership | Builds trust, supports debrief narrative |
| ⚠️ | Provide only partial info | Cautious | Leaves questions unanswered, minor risk |
| ❌ | Defer or delegate without oversight | Disjointed | Undermines authority and clarity |

**Facilitator Prompt:**  
"Executive team, have you reviewed the current legal and media inputs? What is your position on issuing the final briefing?"

**Legal**

**Expectations:**  
• Finalise the breach notification and legal summary.  
• Ensure the messaging aligns with precedent and regulator expectations.  
• Support final media output with accurate, defensible legal framing.

**How they make decisions:**  
• INJ013E (breach draft), INJ013F/R (legal precedent questions), and INJ013T (ministerial report).  
• Use: *Breach Comms Template*, *Post-Breach Reform Guidance*, *Legal Risk Matrix*.

**Key Decision: Approve and Release Breach Notification?**  
• **Trigger:** INJ013E (draft), INJ013F/R (precedent disputes), INJ013T (govt requirement)  
• **Policy:** *Breach Disclosure Protocol, Step 5*

| **OptionDescriptionImplicationScore** |  |  |  |
| --- | --- | --- | --- |
| ✅ | Approve with compliance references | Clear & compliant | Mitigates exposure, matches insurance reqs |
| ⚠️ | Delay pending executive alignment | Coordinated | May delay stakeholder trust |
| ❌ | Reject or rework without timing plan | Risky | Seen as avoidance, legal vulnerability |

**Facilitator Prompt:**  
"Legal team, is your breach notification aligned with precedent and insurance expectations? Are you approving release or awaiting Executive instruction?"

**Technical**

**Expectations:**  
• Complete forensic review and identify final technical vulnerabilities.  
• Support Legal and Operations with validated artefacts.  
• Confirm audit evidence is tagged and timestamped for export.

**How they make decisions:**  
• INJ013A (access to audit logs), INJ013C (cron job), INJ013D (unauthorised badge access).  
• Use: *Forensics Summary Template*, *Audit VM Dashboard*, *Containment Guide – Section 5*.

**Key Decision: Submit Final Technical Report and Log Evidence?**  
• **Trigger:** INJ013A (audit logs), INJ013I (tagging reminder)  
• **Policy:** *Incident Reporting Guide, Section 5.0*

| **OptionDescriptionImplicationScore** |  |  |  |
| --- | --- | --- | --- |
| ✅ | Complete, timestamp, and submit findings | Audit-ready | Ensures continuity into real response process |
| ⚠️ | Submit partial or raw logs | Incomplete | May complicate later review |
| ❌ | Withhold or ignore logging requirement | Irresponsible | No handover record |

**Facilitator Prompt:**  
"Tech team — have you compiled your final forensic logs? Are they validated and ready for export?"

**Operations**

**Expectations:**  
• Secure physical areas and complete operations log for handover.  
• Assess procedural breakdowns (e.g. crane override) and document lessons.

**How they make decisions:**  
• INJ013B (crane override), INJ013D (access attempt), INJ013N (crew confusion).  
• Use: *Ops After-Action Checklist*, *Access Control Summary*, *Ops Closure Procedure Part B*.

**Key Decision: Finalise Operations Log and Access Summary?**  
• **Trigger:** INJ013B (override failure), INJ013J (brief log request)  
• **Policy:** *Ops SOP – Closure Phase*

| **OptionDescriptionImplicationScore** |  |  |  |
| --- | --- | --- | --- |
| ✅ | Provide full handover with timeline | Comprehensive | Supports insurance/legal use |
| ⚠️ | Partial handover, ops notes only | Limited | Reduces detail, some risk |
| ❌ | Skip formal log | Non-compliant | Undermines closure, frustrates debrief |

**Facilitator Prompt:**  
"Ops team — have you handed over all access and operations data? What are your closure steps?"

**Media / Communications**

**Expectations:**  
• Finalise external messaging with CEO and Legal input.  
• Consider holding or modifying statement based on internal alignment.

**How they make decisions:**  
• INJ013G (public tweet), INJ013H (journalist inquiry), INJ013Q (advice to delay).  
• Use: *Comms Summary Template*, *Crisis Comms SOP – Section 6*.

**Key Decision: Issue Final Media Statement Now or Post-Debrief?**  
• **Trigger:** INJ013H (media deadline), INJ013Q (CEO advice), INJ013G (public pressure)  
• **Policy:** *Media SOP – Final Response*

| **OptionDescriptionImplicationScore** |  |  |  |
| --- | --- | --- | --- |
| ✅ | Issue coordinated final summary | Controlled | Ends narrative, promotes transparency |
| ⚠️ | Hold until full internal wrap-up | Safe | No error risk but slower clarity |
| ❌ | Refuse or delay indefinitely | Risky | Allows external narrative to grow |

**Facilitator Prompt:**  
"Media team — are you aligned with Legal and CEO for a final release? Do you plan to issue a summary or delay?"

**Incident Coordinator**

**Expectations:**  
• Close out the master log, tag all critical actions, and prepare for debrief.  
• Ensure legal, executive, and technical decisions are traceable.

**How they make decisions:**  
• INJ013I (log tagging reminder), INJ013J (briefing request), INJ013T (govt report).  
• Use: *Final Log Export Tool*, *Briefing Summary Framework*, *Incident Log SOP – Step 6*.

**Key Decision: Close Incident Log with All Tagged Entries?**  
• **Trigger:** INJ013I (reminder), INJ013T (ministerial report)  
• **Policy:** *Incident Log Closure Protocol*

| **OptionDescriptionImplicationScore** |  |  |  |
| --- | --- | --- | --- |
| ✅ | Close log with all entries tagged | Best practice | Supports team reflection and scoring |
| ⚠️ | Leave log open, collect more post-phase | Flexible | Debrief slightly harder to control |
| ❌ | Forget or skip log export | Breakdown | No continuity for learning or audit |

**Facilitator Prompt:**  
"Coordinator — have you finalised and exported the incident log? Have all team decisions been properly tagged?"