**Phase 1: Disruption Emerges (T+0 to T+30)**

**Overview**

Phase 1 marks the beginning of the coordinated cyber-physical disruption at Southgate Maritime Terminal. The situation appears subtle at first—minor anomalies across AIS, routing, and CCTV systems—but will rapidly expose underlying vulnerabilities and test the teams’ readiness.

Participants will initially be unsure if this is a real incident or just noise. As system failures overlap with expired contingency documents and operational safety concerns, teams will need to begin logging incidents, escalating decisions, and initiating cross-team communication. The phase is designed to simulate uncertainty, requiring judgement, prioritisation, and early use of policy documents.

Injects are delivered at 10-minute intervals, with embedded noise to create operational realism. Teams are not expected to resolve the incident, but must initiate the incident logging process, align on early interpretations, and decide whether escalation is required.

**P1-1: T+0 to T+10**

* INJ001A: Email from Routing Coordinator reporting delayed packet routing to ship manifest system. (Resource: VM-Email)
* INJ001B: Email from Network Monitoring Team reports outbound packet queue spike at Node-04. Urgent trace requested. (Resource: VM-Email)
* INJ001C (Noise): Email – HR reminder: Code of Conduct Acknowledgment overdue. (Resource: VM-Email, Legal, Executive)
* INJ001D (Noise): Log – VM-TempMonitor: Low battery warning on container sensor 12B. (Resource: VM-Logs, Technical)
* INJ001E: Email from Angela Poole, Head of External Affairs, to Media Team. Visibility spike on MarineTracker – prepare holding statement. (Resource: VM-Email)
* INJ001F: Email from Nick Menon, Group Risk & Insurance, to Legal Team. Delay media response due to insurance clause exposure. (Resource: VM-Email)

**P1-2: T+10 to T+20**

* INJ002A: AIS dashboard hides Ship\_Alpha. (Resource: VM-AIS)
* INJ002B: Email from Policy Officer questioning expired contingency documentation. (Resource: VM-Email)
* INJ002C (Noise): Email – Dock Supervisor: "Can we get a new coffee machine on Berth 3?" (Resource: VM-Email, Operations)
* INJ002D (Noise): Email – Media Team: "Do we have old PR photos of Ship\_Alpha arriving?" (Resource: VM-Email, Media)
* INJ002E (Noise): Log – VM-Email: Delivery report failed for message to admin@port. (Resource: VM-Logs, Technical)

**P1-3: T+20 to T+30**

* INJ003A: CCTV blackout triggered on dashboard. (Resource: VM-CCTV Dashboard)
* INJ003B: Email from Dock Supervisor reporting CCTV blind zone on west perimeter. (Resource: VM-Email)
* INJ003C (Noise): Email – Policy Alert: Staff policy 4.7 updated – Non-critical PPE update. (Resource: VM-Email, Legal, Operations)
* INJ003D (Noise): Email – IT Support: Password rotation reminder for Group Admins. (Resource: VM-Email, Technical)
* INJ003E (Noise): Email – HR: "Staff leave report is broken again…anyone else?" (Resource: VM-Email, Executive, Legal)
* INJ003F: Email from Frank Cossar, Dockmaster, to Ops Team. CCTV blackout dangerous – halt ops if not resolved. (Resource: VM-Email)
* INJ003G: Email from Harjit Mann, Tech Support Analyst, to Tech Team. Node-04 isolation will disrupt CCTV relays. (Resource: VM-Email)

Facilitators should ensure that injects are delivered via the appropriate virtual environment channels (e.g., VM-AIS, VM-Email, VM-Logs, VM-CCTV) and that noise injects are indistinguishable in format from core scenario triggers. Teams should begin realising the pattern of subtle-but-critical disruptions, supported by the Incident Coordinator prompting formal logs by the end of this phase.

**Team Expectations and Decisions – Phase 1**

**Executive**

**Expectations:**

* Monitor initial reports across technical and operational domains.
* Conduct early team check-ins to establish a shared understanding.
* Evaluate whether escalation to formal crisis status is warranted.

**How they make decisions:**

* Receive direct briefings from Legal (e.g. expired contingency) and Technical (AIS/network anomalies).
* Use the Crisis Communications SOP and Escalation Tree from the Policy Binder.
* Refer to injects: INJ001A/B (routing/network), INJ002A/B (AIS & documentation), INJ003A/B (CCTV blind zone).

**Key Decision: Escalate Incident to Crisis Response?**

* **Trigger:** Multiple system disruptions or invalid contingency planning (e.g. expired documentation, unexplained network activity).
* **Policy:** Crisis Escalation Tree, Step 1 — formal crisis status includes:
  + Notification of all team leads
  + Shift to scheduled inter-team updates
  + Activation of Comms SOP and spokesperson appointment

| **Option** | **Description** | **Implication** | **Score** |
| --- | --- | --- | --- |
| ✅ Initiate full crisis protocol (notify leads, activate comms) | Proactive coordination | Enables scenario-wide planning, unlocks structured support | +10 |
| ⚠️ Delay escalation, request more data | Conservative approach | Risks lag in structured response and timeline misalignment | +2 |
| ❌ Treat incident as isolated/minor | Passive inaction | Visibility gaps grow, downstream teams misaligned | -6 |

**Facilitator Prompt (if needed):**  
"Executive team, please summarise your current position, any formal decisions made, and intended next steps."

**Legal**

**Expectations:**

* Identify legal exposure due to expired contingency documentation.
* Start an internal compliance log capturing known risks or inaction.
* Flag issues early if they may later affect insurer reporting or regulatory compliance.

**How they make decisions:**

* INJ002B (policy officer email) alerts to an expired contingency plan.
* Legal reviews this using:
  + Legal Risk Flowchart
  + Breach Disclosure Checklist
* Refer to injects: INJ002B (expiry alert), INJ001B (network concern).

**Key Decision: Act on Expired Contingency Document?**

* **Trigger:** INJ002B identifies policy failure.
* **Policy:** Breach Policy, Section 3.2 — delaying could impact coverage or later audit review.

| **Option** | **Description** | **Implication** | **Score** |
| --- | --- | --- | --- |
| ✅ Escalate to Executive and advise workaround | Risk managed | Prompts correction, protects from exposure | +8 |
| ⚠️ Monitor issue but delay escalation | Cautious | Limited visibility, insurer timeline risk | +2 |
| ❌ Ignore the issue | Negligent | No documentation trail, vulnerable in review | -5 |

**Facilitator Prompt (if needed):**  
"Legal team, how are you handling the expired contingency reference in the internal policy email? Are you notifying Executive or holding off?"

**Technical**

**Expectations:**

* Investigate anomalies in AIS display and network traffic from Node-04.
* Coordinate with Ops to confirm operational impact.
* Maintain technical log of actions and notify Executive of containment decisions.

**How they make decisions:**

* Use VM-AIS to identify ship disappearance (INJ001A).
* Read INJ001B network alert from Monitoring team.
* Refer to Technical Containment Guide, specifically:
  + “Signal Anomaly Response”
  + “Node Overload Procedure”
* Coordinate with Incident Coordinator via shared logging tools.
* Refer to injects: INJ001A (AIS anomaly), INJ001B (packet queue spike), INJ002E (email delivery failure).

**Key Decision: Isolate Node-04 to contain network risk?**

* **Trigger:** INJ001B Network Monitoring Alert
* **Policy:** Containment Guide §2.1 — Node isolation should occur if anomalous traffic exceeds threshold.

| **Option** | **Description** | **Implication** | **Score** |
| --- | --- | --- | --- |
| ✅ Isolate Node-04, notify Ops/Exec | Preventive | Limits potential compromise and preserves diagnostics | +9 |
| ⚠️ Monitor without action | Passive | Delays response, may allow issue to spread | +3 |
| ❌ Take no action, assume false positive | Risky | Leaves system exposed, reduces trust in technical leadership | -7 |

**Facilitator Prompt (if needed):**  
"Technical team — is Node-04’s behaviour within expected parameters, or do you see a case for isolation? Have you logged your response?"

**Operations**

**Expectations:**

* Investigate dockside visibility and safety issues related to CCTV loss.
* Assess if AIS loss may affect ship routing or terminal operations.
* Coordinate with Tech to determine if issues are isolated or systemic.

**How they make decisions:**

* INJ003B from the dock supervisor raises concern about CCTV coverage.
* Liaise with Technical to confirm operational implications of INJ001A and INJ003A.
* Use internal alerts from VM-CCTV and Portnet email system.
* Refer to Downtime Impact Estimator and Ops SOP §4.3.

**Key Decision: Restrict Access to CCTV-Impacted Areas?**

* **Trigger:** INJ003B dock supervisor report + known CCTV disruption.
* **Policy:** Ops SOP §4.3 — mandatory safety protocols during sensor outages.

| **Option** | **Description** | **Implication** | **Score** |
| --- | --- | --- | --- |
| ✅ Restrict access, notify Exec | Safety-first | Reduces risk, aligns with duty of care and policy | +8 |
| ⚠️ Monitor zone, act only if more reports emerge | Neutral | Maintains access, but may delay response | +1 |
| ❌ Ignore issue, keep operations normal | Negligent | Elevated safety risk, possible liability | -6 |

**Facilitator Prompt (if needed):**  
"Ops team — has the CCTV blind spot impacted your area’s safety procedures? What access changes, if any, have you made?"

**Media / Communications**

**Expectations:**

* Prepare internal messaging in case incident becomes public.
* Ensure coordination with CEO, Legal, and Executive in real-time.
* Anticipate questions or coverage based on social trends and internal leaks.

**How they make decisions:**

* Use Public Messaging Templates and Comms SOP from Policy Binder.
* Consider cumulative signals: contingency gaps (INJ002B), AIS outage (INJ001A), CCTV report (INJ003B), and noise email on PR photos (INJ002D).

**Key Decision: Prepare Draft Holding Statement?**

* **Trigger:** Multi-team issue detection + public narrative risk.
* **Policy:** Crisis Communications SOP, Section 2

| **Option** | **Description** | **Implication** | **Score** |
| --- | --- | --- | --- |
| ✅ Draft holding line with legal input | Proactive | Prepared for media escalation, shows readiness | +7 |
| ⚠️ Wait until something is public | Passive | May delay response under pressure | +1 |
| ❌ Take no action | Unprepared | Poor response time later | -4 |

**Facilitator Prompt (if needed):**  
"Media team — are you coordinating with Legal to pre-empt messaging? Do you have a statement ready if this goes public?"

**Incident Coordinator**

**Expectations:**

* Establish and maintain structured timeline of events.
* Track team responses and log key decisions across all roles.
* Support Legal and Executive with policy and timestamped artefacts.

**How they make decisions:**

* Begin logging with INJ001A (AIS anomaly) and INJ002A/B (AIS and expired contingency references).
* Collect artefacts from VM-Email, VM-AIS, and network logs.
* Reference Incident Log Template and Coordinator Handbook, Page 1.
* Note noise: INJ003E (HR email) may serve as distraction.

**Key Decision: Start Formal Incident Log Now?**

* **Trigger:** INJ002A/B (documentation failure), INJ001A/B (multiple system impacts).
* **Policy:** Coordinator Handbook, Page 1 — recommends logging begins once multi-role activity is confirmed.

| **Option** | **Description** | **Implication** | **Score** |
| --- | --- | --- | --- |
| ✅ Begin timeline logging and tag injects | Best practice | Enables scoring, improves debrief, supports all teams | +9 |
| ⚠️ Wait for clearer signal from Exec | Cautious | Delays log by ~15 mins, minor record issues | +2 |
| ❌ Log nothing until Phase 2 | Poor practice | Missed actions, lost debrief value | -5 |

**Facilitator Prompt (if needed):**  
"Coordinator — is your incident timeline active? Have you started tagging role actions and injects?"