# Crisis and Incident Management – Crisis Escalation Tree

**Purpose:**  
To provide a clear escalation pathway for determining when an operational anomaly becomes a formal organisational crisis requiring structured response coordination.

## Initial Trigger Points (Any One of These)

Watch for these early indicators. If any apply, initiate Step 1 below:

* Multiple unexplained anomalies across operational or IT systems  
  *(e.g. vessel tracking outage, surveillance feed failure)*
* Expired or invalid contingency or compliance documentation  
  *(e.g. outdated breach plans or contracts referenced by other teams)*
* External visibility begins to emerge  
  *(e.g. social media post, journalist contact, third-party email inquiry)*
* Disruption to logistics or safety systems  
  *(e.g. misrouted container traffic, crane or terminal access issues)*
* Formal requirement to engage legal, insurer, regulator, or stakeholders

## Escalation Tree

**Step 1: Situation Review**

* Convene a 5-minute check-in with CEO, Legal, Tech, and Ops leads
* Coordinator begins or updates the incident log
* Ask:
  + Is the problem spreading?
  + Are other teams affected?
  + Has anyone outside the organisation become aware?

**Step 2: Escalation Thresholds**

* **Threshold A – Localised Disruption:**
  + Issue is contained within one or two teams
  + No safety, legal, or reputational impact yet
  + Handled via routine team-level SOPs
  + **Risk level:** Low (Class C)
* **Threshold B – Internal Disruption with External Risk:**
  + Problem crosses into multiple teams or unclear root cause
  + Visibility increasing outside (e.g. media contact, vendor chain implications)
  + Safety, compliance, or continuity concerns surfacing
  + **Action:** Activate limited structured response (lead appointed, internal updates)
  + **Risk level:** Moderate (Class B)
* **Threshold C – Full Crisis:**
  + Operational or legal breach confirmed or escalating rapidly
  + Coordinated, cross-role response now required
  + Reputation and stakeholder trust at risk
  + **Action:** Trigger full Crisis Protocol (see below)
  + **Risk level:** High/Critical (Class A)

## Activation Protocol (Threshold C)

If Threshold C is met:

1. **Escalation must be authorised by CEO or delegated Crisis Manager**
2. **Notify all team leads immediately**
3. **Incident Coordinator launches master incident log and timestamps events**
4. **Appoint official spokesperson** (usually CEO or Media Lead)
5. **Use Crisis Communications SOP and templates for messaging**
6. **Begin 30-minute update cadence with leadership / Workshop Control**
7. **Capture artefacts for debrief, legal, insurer, and audit purposes**

🔍 *Scenario Guidance Example:*  
If ship tracking has failed, multiple teams have flagged issues, and media has reached out, escalate to Threshold C.

## De-escalation Criteria

* Situation is fully contained and under mitigation
* Public/media exposure is under control or resolved
* Executive team agrees formal crisis mode can end

**Action:** Use the Executive Crisis Wrap Guide to close out

## Notes

* All escalation decisions must be tagged in the log
* Reference Enterprise Risk Register to align classification
* Coordinator should keep running inject timeline linked to thresholds

**Escalation Authority:** CEO or delegated Incident Commander  
**Document Reference:** CIM-01  
**Version:** 1.2  
**Approved by:** Executive Lead, Risk & Compliance