INCIDENT_COORDINATOR_QUESTIONS

SOUTHGATE TERMINAL

Facilitator Questions - INCIDENT COORDINATOR

75-Minute Cyber Crisis Exercise

PURPOSE

These questions help facilitators guide and assess the Incident Coordinator's multi-team coordination, information synthesis, and crisis orchestration throughout the exercise.

TIMING OPTIONS

- **Option A**: Ask questions every 10 minutes for continuous assessment
- **Option B**: Ask at phase transitions (T+30, T+60, T+90)
- **Option C**: Ask at coordination complexity peaks

PHASE 1: Incident Activation & Setup (T+0 to T+30)

P1-1 Questions (T+0 to T+10)

Question: "Have you initiated your incident log? Are you tracking team responses?"

Look for: - Coordination hub establishment - Documentation system setup - Initial team contact

Notes: _____ _____
_____ _____

P1-2 Questions (T+10 to T+20)

Question: "Are you actively logging team actions and requesting summaries? Which teams have responded?"

Look for: - Active information gathering - Team response tracking - Communication rhythm

Notes: _____ _____
_____ _____

P1-3 Questions (T+20 to T+30)

Question: "Have you begun the Situation Update Document? Have all teams provided clear action summaries?"

Look for: - Information synthesis - Gap identification - Update quality

Notes: _____ _____
_____ _____

PHASE 2: Multi-Domain Crisis Management (T+30 to T+60)

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

Question: "Are you documenting ongoing impacts? Are you tracking cross-team coordination clearly?"

Look for: - Impact assessment - Dependency tracking - Resource conflicts

Notes: _____ _____
_____ _____

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

Question: "Are critical decisions logged accurately? Is the mid-scenario update prepared?"

Look for: - Decision documentation - Timeline accuracy - Executive briefing readiness

Notes: _____ _____ _____ _____

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

Question: "Have you prepared the detailed incident status report? Is executive review ready?"

Look for: - Report comprehensiveness - Key decision highlighting - Escalation recommendations

Notes: _____ _____ _____ _____

PHASE 3: Peak Complexity Coordination (T+60 to T+70)

P3-1 Questions (T+60 to T+70)

Question: "Are you tracking escalations across teams clearly?"

Look for: - Multi-team escalation management - Priority conflicts resolution - Resource allocation

Notes: _____ _____ _____ _____

PHASE 4: Resolution & Reporting (T+90 to T+120)

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

Question: "Have all teams consolidated and verified their documentation? Are final reports accurate?"

Look for: - Documentation collection - Consistency verification - Gap identification

Notes: _____ _____
_____ _____

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

Question: "Have final reports been validated for alignment and accuracy? Any outstanding concerns?"

Look for: - Cross-team alignment - Unresolved issues - Lessons learned compilation

Notes: _____ _____
_____ _____

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

Question: "Is your documentation comprehensive and ready for the final debrief?"

Look for: - Master timeline completeness - Decision audit trail - Debrief preparation

Notes: _____ _____
_____ _____

OVERALL ASSESSMENT CRITERIA

Coordination Effectiveness

- [ ] Clear communication established
- [ ] Information flow maintained
- [ ] Team conflicts resolved
- [ ] Resources optimised

Information Management

- [ ] Comprehensive logging
- [ ] Timely synthesis
- [ ] Accurate reporting
- [ ] Gap identification

Crisis Orchestration

- [ ] Appropriate escalation
- [ ] Priority management
- [ ] Decision facilitation
- [ ] Timeline maintenance

GENERAL OBSERVATIONS

Coordination Strengths: _____

_____ _____

Key Challenges Managed: _____

_____ _____

Information Flow Quality: _____

_____ _____

Improvement Opportunities: _____

_____ _____

Facilitator: _____ **Date:** _____ **Exercise ID:** _____