
Security Incident Handling: Triage, Evidence Preservation and Case Closure Training Course

20 – 24 September 2027
New York





Security Incident Handling: Triage, Evidence Preservation and Case Closure Training Course

Ref: 356_22597 **Date:** 20 – 24 September 2027 **Location:** New York **Fees:** 7900 GBP

Programme Summary

Security incident handling, covering triage, evidence preservation and case closure, is the subject of this five-day training course for heads of security, investigations and corporate security managers at a managerial level, ending in a handling plan for one organisation. Incidents lose their value as evidence when judged late, escalated unevenly and closed without a clear record. The programme moves from principles and inquiry standards, through diagnosis of triage and evidence risk, to response and inquiry design, then to reporting, closure and a worked plan. Mars Training Centre UK delivers this programme in security incident handling.

The Business Case

When security incidents are handled case by case, with no shared severity scale and no fixed route for evidence, organisations answer similar events differently and struggle to defend conclusions. Leaders who set triage rules and require closure reviews can show how each case was decided.

- Response Delay: Falls as severity scales and escalation routes are agreed in advance.
- Evidence Loss: Reduces as preservation and custody steps follow one protocol.
- Repeat Incidents: Decline as root causes and lessons are recorded and acted on at closure.

Principles and Evidence Base

- ISO/TS 37008 principles of independence, confidentiality, objectivity and proportionality: These shape the inquiry statement and the handling rules built in Session 1.
- ISO/TS 37008 guidance on planning and conducting internal investigations: It frames the preservation checklist and inquiry plan designed in Session 3.
- ISO/TS 37008 guidance on reporting and closing internal investigations: It informs the report template and closure criteria developed in Session 4.

Intended Participants

- Security leaders who decide how incidents are classified, escalated and resourced.
- Investigations managers who commission inquiries and sign off their findings.
- Corporate security managers who run first response and preserve material at the scene.
- Legal and compliance leads who rely on incident records and inquiry reports.

The programme serves corporate security, financial institutions and industrial operators.



Learning Outcomes

1. Participants will be able to evaluate an organisation's incident handling against international guidance on internal investigations.
2. Participants will be able to diagnose delays, misjudged severity and evidence risks in the incident record.
3. Participants will be able to construct triage, escalation and evidence preservation protocols.
4. Participants will be able to design an inquiry plan with scope, independence and confidentiality safeguards.
5. Participants will be able to appraise incident and inquiry reports for evidence, root cause and clarity.
6. Participants will be able to justify a handling plan and its indicators to a head of security.

Programme Structure

Day 1: Security Incident Handling Principles and Inquiry Standards

Who decides how a security incident is handled, and under which principles is it inquired into?

- ISO/TS 37008 Principles Review
- Incident Category and Severity Scale
- Roles and Escalation Authority Map
- Inquiry Independence and Confidentiality Statement
- Incident Definition and Reporting Brief

Day 2: Diagnosing Incident Flow, Triage and Evidence Risk

Where do incidents stall, get misjudged or lose their evidence before an inquiry begins?

- Incident Log Sample Review
- Triage Decision Audit
- Escalation Delay Analysis
- Evidence Loss Risk Check
- Reporting Channel Coverage Review

Day 3: Designing Response, Evidence Preservation and Inquiry Planning

How are an incident secured, its evidence kept intact and an inquiry scoped?

- Triage and Escalation Protocol
- Scene and Evidence Preservation Checklist
- Chain of Custody Log
- Inquiry Scope and Plan Template
- Interview Planning Sheet



Day 4: Reporting, Closure and Learning

How does an inquiry become a report, and how is a case closed and learned from?

- Findings and Evidence Matrix
- Incident and Inquiry Report Template
- Root Cause Analysis Chart
- Case Closure Review
- Lessons Learned Register

Day 5: Applying Security Incident Handling in One Organisation

Is the handling plan ready for a head of security to adopt?

- Applying the Session 2 Triage Audit to the Chosen Team
- Testing the Session 3 Preservation Checklist on a Live Scenario
- Checking the Session 4 Report Against Closure Criteria
- Setting Handling Indicators for the Team
- Completing the Security Incident Handling Plan

Methodology

The programme uses structured exercises on anonymised incident files from corporate security, industrial and financial settings. Participants work in small teams as incident lead, inquiry manager and client, and take one incident from first report to closure.

- Suggested activity: Triaging a set of incident reports and explaining each severity rating.
- Suggested activity: Listing the evidence at risk in a scenario and ordering the steps that protect it.
- Suggested activity: Rewriting a closure note so that findings, root cause and actions are plain.

Capstone Output

Each participant completes a security incident handling plan for one organisation. It holds a severity scale, a triage protocol, an evidence and custody routine, an inquiry plan template, a closure standard and handling indicators. The plan is used to brief a head of security and to review the next incident.

Frequently Asked Questions

Is security incident handling suitable for managers who do not carry out inquiries themselves?

Yes. Security incident handling is set at managerial level and assumes you direct or rely on inquiries, not that you conduct interviews yourself.



Which standard does security incident handling rest on in this training?

Security incident handling rests on ISO/TS 37008 and its guidance on planning, conducting, reporting and closing internal investigations, including independence, confidentiality, objectivity and proportionality.

How is the plan from security incident handling used at work?

You use the security incident handling plan to brief a head of security, set triage and evidence rules and review how each case is closed.

How does security incident handling differ from a programme on cyber incident response?

Security incident handling centres on corporate and physical security incidents, evidence and internal investigations, while a cyber incident response programme centres on containing attacks on systems and networks.