Cyber Incident Response for Business Professionals Training Course

4 – 8 January 2027
San Diego

AGILE LEADERS
Training Center

Cyber Incident Response for Business Professionals Training Course

Ref: 1687_226861 **Date:** 4 – 8 January 2027 **Location:** San Diego **Fees:** 14000 Euro

Overview

Cyber Incident Response for Business Professionals Training Course is a one-week foundation course for business leaders and response partners, who leave with a Business Cyber Incident Coordination Pack. The course connects incident governance, roles, escalation, decision rights, continuity priorities, stakeholder communications, evidence-preservation awareness, recovery authorization, tabletop exercises and post-incident improvement. Participants practice cross-functional decisions without entering digital forensics or tool configuration. Agile Leaders Training Center develops practical cyber incident response for business coordination skills.

Who Should Attend

- Teams responsible for business leadership and high-impact incident decisions
- Teams responsible for operational continuity and service recovery priorities
- Teams responsible for risk, legal, human resources and supplier coordination
- Teams responsible for internal, customer and public communications
- Teams responsible for cybersecurity governance and incident liaison

The course assumes participants can interpret business impacts and organizational responsibilities at work, and leaves out digital forensics, malware analysis, technical containment tools and legal advice.

Departments and Industries

The course supports departments that coordinate business decisions during cyber incidents across service environments.

- Executive leadership and business operations
- Risk, compliance and corporate governance
- Communications, legal and human resources
- Financial services, healthcare and digital commerce
- Manufacturing, utilities and infrastructure services

Learning Objectives

By the end of this course, participants will be able to:

- Build incident roles and escalation structures
- Prioritize business services and recovery decisions
- Use executive decision and situation-report tools
- Evaluate stakeholder communication needs
- Apply evidence-preservation and coordination controls
- Analyze exercise findings and improvement actions

Course Agenda

Day 1: Incident Governance and Readiness

- NIST SP 800-61 Rev. 3 Response Lifecycle Map
- Business Incident Classification and Severity Matrix
- Incident Roles, Deputies and Decision-Rights Chart
- Contact, Supplier and Escalation Directory
- Readiness, Authority and Resource Checklist

Day 2: Impact and Response Decisions

- Business Service Impact and Dependency Map
- Minimum Viable Operations Priority Matrix
- Containment Decision Consequence Canvas
- Executive Situation Report and Decision Log
- Action Owner, Deadline and Assumption Tracker

Day 3: Communications and Coordination

- Stakeholder Communication Needs Matrix
- Internal Briefing and Message Approval Workflow
- Customer, Supplier and Partner Update Template
- Legal, Human Resources and Communications Engagement Map
- Evidence Preservation and Information-Sharing Checklist

Day 4: Recovery and Improvement

- Recovery Authorization and Service Restoration Gate
- Backup Integrity and Return-to-Operation Checklist
- Recovery Progress and Residual-Risk Dashboard
- Incident Closure and Documentation Criteria
- After-Action Review and Improvement Register

Day 5: Tabletop Practice and Capstone

- Exercise: Classify an Incident and Activate Roles
- Exercise: Prioritize Services and Record Decisions
- Exercise: Coordinate Stakeholder Communications
- Exercise: Authorize Recovery and Capture Lessons
- Capstone: Business Cyber Incident Coordination Pack

Practical Exercises

The course uses suggested activities based on service disruption, data exposure and supplier-compromise scenarios.

- Suggested activity: assign roles, deputies and escalation paths for a developing incident
- Suggested activity: compare containment options against operational and stakeholder impacts
- Suggested activity: prepare a situation report and coordinated stakeholder update
- Suggested activity: conduct a tabletop review and prioritize improvement actions

FAQs

Who suits cyber incident response for business training and what does it assume?

Cyber incident response for business training suits managers, department heads, risk coordinators, communications teams and business partners to technical responders. It assumes basic familiarity with business services and responsibilities while excluding forensic and tool-level work.

How does cyber incident response for business training differ from technical incident handling?

Cyber incident response for business training focuses on governance, authority, impacts, communications, continuity, recovery and lessons. Technical incident handling usually concentrates on detection evidence, system analysis, containment execution, eradication and forensic methods.

Why are decision logs important in cyber incident response?

Decision logs record what was known, which options were considered, who authorized an action and which assumptions shaped it. They support coordination, handovers, accountability and later review without replacing technical evidence.

What should a cyber incident tabletop exercise test?

A cyber incident tabletop exercise should test activation, roles, escalation, service priorities, decision authority, communications, supplier coordination, recovery gates and documentation. Its purpose is to expose unclear responsibilities and assumptions before a real incident.

AGILE LEADERS
Training Center

Conclusion

Participants take back a Business Cyber Incident Coordination Pack containing role charts, escalation paths, impact priorities, situation reports, decision logs, communication tools, recovery gates and improvement actions. The pack gives business and technical teams a shared coordination structure under pressure. It also turns tabletop findings into assigned readiness improvements.