

COURSE BROCHURE

Cyber Incident Response and Crisis Management

Professional Training Course

Skillslab Training Provider

Skills for Tomorrow's World 



Course Description

Course Overview

The **Cyber Incident Response and Crisis Management** course is a comprehensive, theory-focused program designed to equip public and private sector managers with the knowledge and leadership perspective required to respond effectively to cyber incidents and technology-driven crises. As organizations become increasingly dependent on digital systems, cyber incidents are no longer purely technical events; they are organizational crises that demand structured leadership, clear decision-making, and coordinated response at the management level.

This course is especially relevant for new managers and supervisors who may be required to lead teams, communicate with stakeholders, or make time-critical decisions during a cyber incident without being technical specialists. Positioned within **leadership training for new managers**, the program emphasizes governance, roles and responsibilities, crisis coordination, and executive-level response rather than hands-on technical remediation. Participants gain a practical understanding of how cyber incidents escalate into organizational crises and how leaders can mitigate impact, protect reputation, and restore operational stability.

Key Outcomes

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

- By the end of this program, participants will be able to understand the nature and types of cyber incidents affecting organizations.
- By the end of this program, participants will be able to distinguish between technical response and managerial crisis leadership roles.
- By the end of this program, participants will be able to explain the stages of cyber incident response at an organizational level.
- By the end of this program, participants will be able to recognize leadership responsibilities during cyber-related crises.
- By the end of this program, participants will be able to support structured decision-making under pressure.

- By the end of this program, participants will be able to identify common risks and escalation points in incidents.
- By the end of this program, participants will be able to strengthen organizational preparedness and resilience.
- By the end of this program, participants will be able to apply leadership principles to post-incident recovery and learning.

Who Should Attend

This course is designed for professionals who hold or are preparing for leadership, supervisory, or coordination roles in organizations where cyber incidents may disrupt operations, including:

- First-time managers and newly appointed supervisors
- Team leaders and department heads
- High-potential employees preparing for leadership roles
- Middle managers responsible for operational continuity
- Business managers overseeing digital or data-driven services
- Staff involved in crisis management or risk oversight

Prerequisites: No prerequisites.

Course Outline by Modules

Day 1: Understanding Cyber Incidents as Organizational Crises

- Overview of cyber incidents and their organizational impact
- Why cyber incidents are leadership and management issues
- Common types of cyber-related disruptions
- Escalation from technical issue to organizational crisis
- Leadership awareness and accountability

Day 2: Cyber Incident Response Frameworks and Roles

- Key phases of cyber incident response
- Organizational roles and responsibilities during incidents
- Leadership versus technical response boundaries
- Decision-making structures and authority

- Managing uncertainty and incomplete information
- Prioritization and rapid decision-making principles
- Supporting teams during crisis conditions
- Ethical and accountability considerations

Day 4: Communication, Stakeholders, and Reputation Management

- Internal communication during cyber incidents
- External communication and stakeholder coordination
- Managing expectations and information flow
- Protecting organizational trust and credibility
- Leadership visibility and messaging during crises

Day 5: Recovery, Learning, and Organizational Resilience

- Transition from response to recovery
- Post-incident review and lessons learned
- Strengthening policies and preparedness
- Building long-term organizational resilience
- Leadership commitment to continuous improvement

Methodology

The **Cyber Incident Response and Crisis Management** course is delivered through a primarily theoretical and structured learning methodology. The focus is on leadership concepts, crisis management frameworks, and organizational response principles rather than technical incident handling or system-level intervention. This makes the program highly suitable for **first-time manager training, management skills training**, and broader leadership development initiatives.

Learning is facilitated through instructor-led explanations, guided discussions, and simplified crisis scenarios relevant to organizational leadership. Interaction includes individual reflection and light group discussions that allow participants to explore leadership challenges without engaging in complex simulations. Practical elements are intentionally minimal and may include short quizzes, basic decision-mapping exercises, or simple communication planning templates completed on a computer. Training materials include summary sheets, a

Participant learning is assessed during the training sessions through short quizzes, guided question-and-answer activities, and recap checks at the end of each day. These in-session assessments are designed to reinforce understanding of cyber incident response concepts and leadership responsibilities without formal testing or technical evaluation.

Organizations may independently assess return on investment using internal performance indicators such as improved crisis readiness, clearer leadership roles during incidents, faster decision escalation, improved communication effectiveness, or manager performance reviews. **Internal measurement is managed by the client organization and is outside the scope of our delivery.** Optional follow-up support or advisory discussions may be arranged upon request.

Instructor Profile

Instructor assignment depends on the delivery date and city. We work with a global pool of trainers. Please contact us to confirm the most suitable available instructor for this course based on schedule and location.

Conclusion

The **Cyber Incident Response and Crisis Management** course provides managers with the leadership insight and structured understanding required to navigate cyber-related crises with confidence and clarity. As part of a **new manager leadership course, leadership fundamentals course, or supervisor leadership program**, this training strengthens decision-making, coordination, and organizational resilience. Organizations seeking effective **leadership development for team leaders**, practical **management skills training**, and a recognized **certificate of completion** are invited to contact us to tailor the delivery format—onsite, online, or blended—with flexible duration options aligned to organizational needs.

Contact Us

For registration inquiries, upcoming dates, or group pricing, please contact us:

Website

www.skillslab-training.com

Email

info@skillslab-training.com

WhatsApp

+966 559 653 447

Generated by Skillslab Training

info@skillslab-training.com | WhatsApp: +966 559 653 447

www.skillslab-training.com