Security Leadership in Crisis and Business Continuity Training Course



23 - 27 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM4847_131288

Course Introduction / Overview:

In today's volatile and interconnected world, the role of a security leader extends far beyond traditional responsibilities. Proactive crisis management and robust business continuity planning are no longer optional but are core strategic imperatives for organizational survival and resilience. This comprehensive training course is meticulously designed to equip security leaders with the advanced skills needed to navigate complex crises, protect critical assets, and ensure operational continuity. Drawing upon established frameworks and contemporary challenges, the program delves into the complete lifecycle of crisis and continuity management. As noted by prominent academic Dr. Denis Fischbacher-Smith in his works on organizational resilience, a successful response is predicated on foresight and rigorous preparation. This course, offered by BIG BEN Training Center, moves beyond theoretical concepts, providing a practical roadmap for developing, implementing, and testing effective plans. Participants will explore concepts from leading literature like "The Definitive Handbook of Business Continuity Management," learning to build a resilient security posture that can withstand disruptions, from cyber-attacks and supply chain failures to natural disasters and reputational threats. This is the definitive program for leaders committed to mastering strategic crisis management and safeguarding their organization's future.

Target Audience / This training course is suitable for:

- Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs).
- Corporate Security Directors and Managers.
- Business Continuity and Disaster Recovery Planners.
- Risk Management Professionals.
- IT Directors and Senior IT Security Managers.
- Operations and Facilities Managers.
- Emergency Response Team Leaders.
- Members of the corporate crisis management team.
- Security consultants and advisors.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Energy, Oil, and Gas.
- Manufacturing and Supply Chain Logistics.
- Retail and Consumer Goods.
- Governmental agencies and public sector bodies.
- Critical Infrastructure Operators.
- Transportation and Aviation.

Target Organizations Departments:

- Corporate Security and Asset Protection.
- Information Security and Cybersecurity.
- Risk Management and Compliance.
- Operations Management.
- Facilities and Physical Security.
- Information Technology (IT).
- Executive Leadership and Strategic Planning.
- Human Resources.
- Legal and Corporate Governance.

Course Offerings:

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

- Develop and implement an integrated crisis management and business continuity framework.
- Conduct a thorough Business Impact Analysis (BIA) to identify critical functions and dependencies.
- Perform comprehensive risk assessments and threat landscape analyses.
- Formulate strategic crisis communication plans for internal and external stakeholders.
- Lead and manage a Crisis Management Team (CMT) effectively during an incident.
- Design and facilitate realistic tabletop exercises and simulation drills.
- Establish clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Integrate cyber and physical security incident response protocols.
- Drive a culture of resilience and preparedness throughout the organization.
- Evaluate and improve existing continuity plans through post-incident reviews.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum engagement and practical application. This course adopts a blended learning approach that combines expert-led instruction with highly interactive and participatory sessions. We believe that adult learning is most effective when participants can directly apply concepts to their own professional contexts. Therefore, the curriculum is heavily based on real-world case studies of major corporate crises, allowing for in-depth analysis of what went right and what went wrong. A significant portion of the training is dedicated to hands-on workshops, including the development of a draft Business Impact Analysis (BIA) and the framework for a crisis communication plan. A key feature is the use of dynamic tabletop exercises and simulations, where participants work in teams to navigate a developing crisis scenario, making critical decisions under pressure. These exercises provide a safe environment to test plans, identify gaps, and refine leadership skills. Group discussions, peer-to-peer feedback sessions, and Q&A with experienced instructors ensure a rich, collaborative learning environment that fosters deep understanding and builds confidence in applying these critical skills.

Course Agenda (Course Units):

Unit One: Foundations of Strategic Crisis and Continuity Management

- Defining the modern crisis and threat landscape.
- The strategic link between crisis management, business continuity, and organizational resilience.
- Understanding the role and responsibilities of a security leader in a crisis.
- Key terminology, standards, and frameworks (e.g., ISO 22301, NIST).
- Establishing a governance structure for crisis and continuity programs.
- Legal, regulatory, and compliance considerations in planning.
- Securing executive buy-in and building a business case for investment.

Unit Two: Risk Assessment and Business Impact Analysis (BIA)

- Systematic approaches to threat identification and risk assessment.
- Conducting a comprehensive Business Impact Analysis (BIA).
- Identifying and prioritizing critical business functions and processes.
- Mapping internal and external dependencies, including supply chain vulnerabilities.
- Determining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- Analyzing the financial and non-financial impacts of disruption.
- Presenting BIA and risk assessment findings to senior leadership.

Unit Three: Developing the Crisis and Continuity Plans

- Structuring the Crisis Management Plan (CMP).
- Developing the Business Continuity Plan (BCP) for critical functions.
- Creating a robust Crisis Communication Plan for all stakeholders.
- Integrating IT Disaster Recovery (DR) plans with the overall BCP.
- Defining roles, responsibilities, and succession plans for the Crisis Management Team (CMT).
- Establishing protocols for incident declaration and plan activation.
- Resource management and logistics planning for a crisis response.

Unit Four: Crisis Response Leadership and Team Management

- Activating the Crisis Management Team (CMT) and Emergency Operations Center (EOC).
- Effective leadership and decision-making under extreme pressure.
- Executing the crisis communication strategy with clarity and empathy.
- Managing information flow and situational awareness.
- Coordinating with first responders, government agencies, and external partners.
- Addressing the human element: employee welfare and psychological support.
- Tactical incident response for both physical and cyber events.

Unit Five: Testing, Maintenance, and Building Organizational Resilience

- Designing and facilitating effective tabletop exercises and drills.
- Conducting full-scale simulations to test plans and team readiness.
- Strategies for plan maintenance, review, and continuous improvement.
- Conducting a post-incident review and capturing lessons learned.
- Embedding a culture of preparedness and resilience across the organization.
- Future-proofing plans for emerging threats and evolving business needs.
- Measuring program effectiveness and reporting on resilience metrics to the board.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How can a security leader balance the need for decisive, top-down command during a crisis with the benefits of collaborative, decentralized problem-solving within their team?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing intently on the strategic leadership dimension of crisis and continuity management, a critical element often overlooked in purely technical training. While many programs teach the mechanics of writing a plan, this course is built around the art and science of leading an organization through turmoil. It moves beyond checklists to cultivate the critical thinking, decision-making, and communication skills that define effective leadership under pressure. A core differentiator is our emphasis on realistic, high-fidelity simulations and tabletop exercises that mirror the complex, ambiguous nature of real-world crises. Participants do not just learn theory; they are immersed in scenarios that test their ability to manage stakeholders, allocate resources, and communicate with confidence. Furthermore, the curriculum uniquely integrates the often-siloed disciplines of physical security, cybersecurity, and business operations into a single, cohesive resilience strategy. The academic rigor, grounded in established frameworks and contemporary research on organizational resilience, ensures that participants leave not just with a plan, but with a forward-looking mindset to build a truly robust and adaptive security posture for their organization.