Strategic Cyber Resilience and Business Continuity Training Course



14 - 18 Dec 2026

Cairo

3700 € (Per Person)

Ref: #CYB2668_272325

Course Introduction / Overview:

In today's hyper-connected digital landscape, the question is not if an organization will face a cyber disruption, but when. This course provides a comprehensive framework for building robust organizational resilience against a spectrum of modern threats. We move beyond traditional disaster recovery to foster a proactive culture of cyber resilience and business continuity management (BCM). This program is meticulously designed to equip professionals with the strategic foresight and practical tools needed to anticipate, withstand, recover from, and adapt to adverse cyber events. Drawing upon established principles from leading experts like Andrew Hiles, editor of "The Definitive Handbook of Business Continuity Management," this training integrates key concepts from risk assessment, incident response, and crisis communication. At BIG BEN Training Center, we believe that true resilience is not just a technical function but a core business strategy that safeguards reputation, maintains customer trust, and ensures operational viability. This course will guide participants through the entire BCM lifecycle, from conducting a business impact analysis to executing recovery strategies and embedding a continuous improvement mindset within their organization.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs).
- Business Continuity and Disaster Recovery Managers.
- IT Directors and Senior IT Managers.
- Risk, Compliance, and Governance Professionals.
- Crisis Management Team Members.
- Operations Managers and Department Heads.
- Information Security Analysts.
- Emergency Planners and Coordinators.
- Senior Executives and Board Members involved in strategic risk.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceutical.
- Information Technology and Telecommunications.
- Energy, Oil, and Gas sectors.
- Governmental agencies and public sector bodies.
- Manufacturing and Supply Chain Logistics.
- Retail and E-commerce.
- Professional Services and Consulting.

Target Organizations Departments:

- Information Technology and Cybersecurity.
- Risk Management and Compliance.
- Operations and Business Units.
- Internal Audit.
- Human Resources.
- Legal and Corporate Governance.
- Facilities Management.
- Corporate Communications and Public Relations.
- Executive Management.

Course Offerings:

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

- Develop and implement a comprehensive business continuity management system (BCMS).
- Conduct a thorough business impact analysis (BIA) to identify critical functions.
- Perform a detailed risk assessment to identify potential threats and vulnerabilities.
- Define and establish recovery time objectives (RTOs) and recovery point objectives (RPOs).
- Design robust incident response and disaster recovery plans (DRPs).
- Integrate cyber resilience principles into the organizational culture and governance structure.
- Lead crisis management and communication efforts during a disruptive event.
- Plan and execute effective business continuity tests and exercises.
- Align business continuity strategies with international standards like ISO 22301.
- Manage third-party and supply chain risks effectively.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring participants can apply learned concepts directly to their professional roles. We employ a blended learning approach that combines expert-led instruction with collaborative and hands-on activities. The course heavily features real-world case studies of cyber incidents and business disruptions, allowing participants to analyze response strategies and outcomes in a controlled environment. A significant portion of the training is dedicated to group workshops and syndicate exercises, including the development of a sample business impact analysis and the drafting of incident response protocols. Interactive sessions, facilitated discussions, and Q&A panels encourage knowledge sharing and peer-to-peer learning. A key component of the course is a simulated tabletop exercise where participants work as a team to navigate a realistic crisis scenario, making critical decisions under pressure. This practical application solidifies understanding and builds confidence. Continuous feedback is provided by the instructor to guide learning and ensure all objectives are met, creating a dynamic and effective educational experience.

Course Agenda (Course Units):

Unit One: Foundations of Organizational Resilience

- Introduction to Cyber Resilience and Business Continuity Management (BCM).
- The relationship between Information Security, BCM, and Disaster Recovery.
- Understanding the BCM lifecycle and its core components.
- Key terminology: RTO, RPO, BIA, and MTPD.
- Introduction to international standards and frameworks (ISO 22301, NIST Cybersecurity Framework).
- The role of leadership and governance in building a resilient organization.
- Establishing a policy and program for business continuity.

Unit Two: Risk Assessment and Business Impact Analysis

- Methodologies for conducting a comprehensive risk assessment.
- Identifying and prioritizing critical business processes and functions.
- The step-by-step process of a Business Impact Analysis (BIA).
- Determining the impact of disruptions on operations, finance, and reputation.
- Mapping interdependencies between processes, applications, and infrastructure.
- Analyzing supply chain and third-party vendor risks.
- Documenting and presenting BIA and risk assessment findings to stakeholders.

Unit Three: Developing Continuity and Response Strategies

- Developing business continuity strategies based on BIA results.
- Designing resilient IT architecture and data recovery solutions.
- Creating a detailed Business Continuity Plan (BCP).
- Formulating a comprehensive Cyber Incident Response Plan (IRP).
- Building a structured Disaster Recovery Plan (DRP) for critical systems.
- Integrating crisis management and communication protocols.
- Defining roles, responsibilities, and activation criteria for response teams.

Unit Four: Crisis Management and Incident Response

- Understanding the phases of crisis management.
- Establishing a command-and-control structure for incident response.
- Effective communication strategies for internal and external stakeholders.
- Managing media relations and protecting brand reputation during a crisis.
- Activating and executing the BCP and IRP.
- Coordinating with law enforcement and regulatory bodies.
- Techniques for damage control and initial impact assessment.

Unit Five: Testing, Maintaining, and Improving Resilience

- The importance of a continuous improvement cycle.
- Planning and designing BCM tests and exercises (e.g., tabletop, simulations).
- Conducting a tabletop exercise to validate plans and team readiness.
- Analyzing test results and identifying gaps for improvement.
- Establishing a plan maintenance and review schedule.
- Embedding a culture of resilience throughout the organization.
- Future trends in cyber threats and business continuity.

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:

In an era of interconnected global supply chains and state-sponsored cyber threats, can any organization truly achieve complete cyber resilience, or is it a perpetual process of mitigation and adaptation?

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

This training course distinguishes itself by adopting a strategic, top-down approach to organizational resilience, moving beyond purely technical disaster recovery solutions. While many courses focus on the IT components of recovery, our curriculum integrates cyber resilience and business continuity as a core leadership and governance function. We emphasize the critical interplay between technology, people, and processes, ensuring participants understand how to build a resilient culture, not just a resilient infrastructure. The program's unique strength lies in its focus on practical application through immersive simulations and real-world case studies, forcing participants to engage in the type of critical thinking and decision-making required during an actual crisis. Furthermore, the content is deeply rooted in established management frameworks like ISO 22301 and NIST, providing a structured, standards-based methodology that can be implemented immediately. We delve into the often-overlooked aspects of crisis communication, stakeholder management, and supply chain risk, offering a truly holistic and 360-degree view of what it takes to protect an organization and ensure its continuity in the face of modern, sophisticated threats.