Digital Resilience and Business Continuity Planning Training Course



19 - 23 Oct 2026

Cairo

3700 € (Per Person)

Ref: #DT7543_273319

Course Introduction / Overview:

In today's hyper-connected world, the line between digital operations and business survival has vanished. Organizations face an ever-expanding landscape of digital risks, from sophisticated cyber-attacks and data breaches to system failures and supply chain disruptions. Proactive digital risk management and robust business continuity planning are no longer optional IT functions but core strategic imperatives for ensuring organizational resilience and long-term viability. This comprehensive course offered by BIG BEN Training Center provides a holistic framework for navigating this complex environment. Drawing on principles articulated by risk management experts like David L. Olson, the curriculum moves beyond theory to practical application. It equips participants with the tools to identify, assess, and mitigate digital threats effectively. Inspired by foundational texts such as "Enterprise Risk Management", this program integrates digital risk management into the broader context of business continuity, ensuring that your organization can not only withstand disruptions but also adapt and thrive in the face of adversity. This training is designed to build a culture of resilience from the ground up, transforming your approach from reactive recovery to proactive strategic preparedness for any digital eventuality.

Target Audience / This training course is suitable for:

- Business Continuity and Disaster Recovery Managers.
- IT Directors, Managers, and Team Leaders.
- Risk, Compliance, and Governance Professionals.
- Information Security (InfoSec) and Cybersecurity Specialists.
- Operations Managers and Department Heads.
- Project Managers involved in critical system implementations.
- Internal and External Auditors.
- Senior Executives (CIOs, CISOs, COOs) responsible for organizational resilience.
- Emergency Planners and Crisis Management Team Members.

Target Sectors and Industries:

- Banking, Financial Services, and Insurance.
- Healthcare and Pharmaceutical sectors.
- Information Technology and Telecommunications.
- Governmental bodies and public sector agencies.
- Manufacturing and Industrial sectors.
- Retail and E-commerce.
- Energy and Utilities.
- Transportation and Logistics.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT) and Cybersecurity.
- Risk Management and Compliance.
- Operations and Business Units.
- Internal Audit and Quality Assurance.
- Executive Leadership and Strategic Planning.
- Facilities and Corporate Security.
- Legal and Corporate Governance.
- Human Resources.
- Procurement and Supply Chain Management.

Course Offerings:

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

- Conduct a comprehensive Business Impact Analysis (BIA) to identify critical functions and dependencies.
- Develop, implement, and maintain a robust Business Continuity Plan (BCP) aligned with ISO 22301 standards.
- Identify, analyze, and evaluate a wide range of digital risks using established frameworks like NIST.
- Formulate effective risk mitigation and treatment strategies to enhance operational resilience.
- Establish clear Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical systems.
- Design and execute effective BCP testing and exercise scenarios, including tabletop and simulation exercises.
- Develop and lead an effective incident response and crisis management team.
- Integrate third-party and supply chain risk management into the business continuity framework.
- Communicate effectively with stakeholders during a crisis to manage reputation and maintain trust.
- Foster a culture of digital resilience and continuous improvement within the organization.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring that participants can immediately apply their learning in a real-world context. We move beyond traditional lectures to create an immersive learning environment built on a foundation of experiential activities. The course heavily utilizes case studies of recent, high-profile digital disruptions and cyber incidents, allowing participants to analyze what went right and what went wrong in real corporate scenarios. A significant portion of the training is dedicated to hands-on workshops and group exercises where participants will collaboratively conduct a mock Business Impact Analysis (BIA), develop core components of a Business Continuity Plan (BCP), and simulate risk assessment processes. Interactive sessions, facilitated discussions, and peer-to-peer learning are central to our approach, encouraging the sharing of diverse experiences and perspectives. Participants will engage in a simulated crisis management tabletop exercise to test their decision-making and communication skills under pressure. Continuous feedback from the instructor ensures that learning is reinforced and that complex concepts are fully understood, creating a dynamic and effective educational experience.

Course Agenda (Course Units):

Unit One: Foundations of Digital Resilience and Business Continuity

- Introduction to Digital Risk Management and Business Continuity Management (BCM).
- Key Terminology: BIA, RTO, RPO, BCP, DRP.
- The Global Threat Landscape and Emerging Digital Risks.
- The Business Case for Investing in Organizational Resilience.
- Understanding International Standards and Frameworks (ISO 22301, NIST).
- The Role of Governance and Leadership in BCM.
- Integrating BCM into the Organizational Culture.

Unit Two: Strategic Digital Risk Assessment and Management

- Identifying Digital Threats, Vulnerabilities, and Assets.
- Qualitative and Quantitative Risk Assessment Techniques.
- Conducting a Comprehensive Risk Analysis.
- Risk Evaluation and Prioritization.
- Developing a Risk Treatment and Mitigation Plan.
- Implementing and Monitoring Risk Controls.
- Introduction to Third-Party and Supply Chain Risk Management.

Unit Three: Conducting the Business Impact Analysis (BIA)

- The Purpose and Scope of the Business Impact Analysis.
- Methodologies for Data Gathering: Interviews, Workshops, and Surveys.
- Identifying and Prioritizing Critical Business Functions and Processes.
- Mapping Dependencies: Systems, People, and Suppliers.
- Determining Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- Analyzing the Impact of Disruptions (Financial, Reputational, Operational).
- Documenting and Presenting BIA Findings to Senior Management.

Unit Four: Developing and Implementing the Business Continuity Plan (BCP)

- Translating BIA Results into Continuity Strategies.
- Structure and Key Components of a Modern BCP.
- Developing Incident Response and Activation Procedures.
- Defining Roles, Responsibilities, and Command Structure (Crisis Management Team).
- Crafting an Effective Crisis Communications Plan for Internal and External Stakeholders.
- Resource Management and Logistics in a Crisis.
- Documenting the Plan and Gaining Stakeholder Approval.

Unit Five: BCP Testing, Maintenance, and Crisis Leadership

- The Importance of a BCP Testing and Exercise Program.
- Types of Tests: Plan Walk-throughs, Tabletop Exercises, and Full Simulations.
- Planning, Executing, and Evaluating a BCP Test.
- Updating the BCP Based on Test Results and Environmental Changes.
- Leading with Confidence During a Crisis.
- Post-Incident Review and Continuous Improvement.
- Future-Proofing Your BCM Program for Emerging Technologies and Threats.

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 pervasive AI, how can a traditional Business Continuity Plan evolve to address systemic, cascading digital failures?

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

This course distinguishes itself by adopting a holistic and strategic perspective, treating digital risk and business continuity not as isolated technical functions but as deeply integrated components of organizational resilience and competitive advantage. While other courses may focus narrowly on creating a BCP document, our curriculum emphasizes the entire lifecycle of resilience, from proactive threat identification and risk assessment to dynamic crisis leadership and post-incident learning. We move beyond theoretical frameworks by immersing participants in practical, real-world scenarios and advanced case studies that reflect the current complex threat landscape, including state-sponsored attacks and sophisticated ransomware incidents. The program's unique value lies in its focus on developing critical thinking and strategic decision-making skills. Rather than just providing templates, we equip leaders to analyze the results of a Business Impact Analysis (BIA) and formulate bespoke continuity strategies that are robust, flexible, and aligned with their specific organizational context. The emphasis on crisis communication and stakeholder management provides a crucial, often overlooked, skill set essential for protecting brand reputation and maintaining trust during a disruptive event. This forward-looking approach ensures participants are prepared not just for today's risks, but for the emerging challenges of tomorrow.