

Disaster Recovery and Business Continuity Planning (Mile2)

Course Number: DRBCP

Length: 4 Day(s)

Certification Exam

This course will help you prepare for the following exams:

- **ABCP:** Associate Business Continuity Planner (DRII-USA)
- **CBCP:** Certified Business Continuity Planner (DRII-USA)

Course Overview

This introductory course has been built upon proven Disaster Recovery Planning and business continuity planning “BCP” methodologies. The course presents information on the latest risks and responses. The class also enhances the business skills needed to identify protection opportunities, justify budget requests to optimize DR processes. Our course is developed on the generally accepted principals and uses the same methods and best practices. Its focus is professional DRBCP - Disaster Recovery & Business Continuity Planning for protection of assets and human life.

Prerequisites

Students taking this course should have:

- A minimum of 12 months experience in risk management, security or facilities management.
- Sound knowledge of business assessment and writing skills.

Audience

This course is intended for Risk Management professionals, Security and Facilities professionals and Project Managers.

Course Outline

- **Module 1 - Initiation and Project Management**
- Initiation and Project Management
- Disaster Recovery
- Business Continuity
- What is a Disaster?
- Disaster Recovery
- Goals
- Who is responsible for BC/DR?
- Purpose of DR/BC Program

- Resistance to Change
- DR/BC Project Management
- DR/BC Planning Model
- Project Initiation Phase
- Functional Requirements Phase
- Change Control
- Recommended Structure
- Team Overview in Project Plan
- Typical functional areas to consider
- Chapter Review
- **Module 2 - Risk Evaluation & Control**
- Risk Evaluation & Control
- Risk Analysis Activities
- Threats to Business Process
- Disaster Categories
- Technical Disaster Scenarios
- Human Disaster Scenarios
- Other Human Disaster Scenarios
- Threats
- Downtime
- Risk Analysis Terminology
- Risk management
- Risk Analysis Activities
- Exposure Inventory
- Business Process Inventory
- Business Process Documentation
- Important Areas to Watch
- Potential Impact on Operations
- Statement of Risk
- ALE Annualized Loss Expenditure or Expectancy
- Annualized Loss Exposure
- Statement of Risk
- Risk Control Definition
- Identifying Existing Controls
- Physical Controls
- Risk Analysis
- Risk Assessment Report
- Compiling a Risk Assessment Report
- Chapter Review
- **Module 3 - Business Impact Analysis BIA**
- Business Impact Analysis BIA
- Business Impact Analysis Terminology
- Objectives of Business Impact Analysis
- Recovery Time Objective RTO
- BIA Phases
- BIA Project Planning

- BIA Tools
- More on BIA
- BIA Analysis Details
- BIA
- Notes on Data Collection
- Notes on Data Analysis
- Data Analysis
- Where does BIA fit into the Process
- Chapter Review
- **Module 4 - Developing Strategies**
- Developing Strategies
- Business Continuity Program
- Strategy Process
- Developing DR/BC Strategies
- DR/BC Specifics
- Selecting Off-Site Storage and Alternate Recovery Site(s)
- Off-Site Storage
- Selecting Vendors for DR/BC Services
- Evaluating Vendors of DR/BC Resources
- Identifying Recovery Strategies for Functional Areas
- More on Recovery Strategies
- Telecommunications Strategies
- Assessing Strategies from BIA
- Cost/Benefit Analysis
- More Continuity Strategies
- Consolidating Continuity Strategies Across the Enterprise
- Consolidating Continuity and Recovery Strategies Across the Enterprise
- Hardware Backup Alternatives
- Continuity Strategy - Hardware Backup Alternatives
- Critical Factors
- Continuity Strategy
- Continuity Strategy - Software Backup Alternatives
- Software Backup Alternatives
- Data Backup Alternatives
- Telecom & Network Alternatives
- Business Continuity
- Continuity Strategy - Insurance
- Evaluate Insurance Terms
- Chapter Review
- **Module 5 - Emergency Preparedness and Response**
- Emergency Preparedness and Response
- Purpose of Emergency Response Procedures
- Emergency Response
- Emergency Response Components
- Develop ER Procedures
- Command and Control

- ER Sources for Assistance
- Chapter Review
- **Module 6 - BC Plan Development and Implementation**
- BC Plan Development and Implementation
- DR/BC Involves
- Planning Considerations
- Planning Methodology
- Scope of Project Plan
- Planning Assumptions
- Planning Responsibilities
- Plan Should Include Key Disaster Scenarios
- Work Plans & Schedules
- Requirements for Plan Elements
- Build Team
- Recovery Restoration Teams
- Steps : Execution Strategy
- Plan Development Phase
- Design & Development Phase
- Organizational Tools
- Organizational Tasks
- Media Control
- Personnel Mobilization
- General Employee Information
- Business Continuity Designates
- Implementation of Planning Process
- Responsibility for Developing Procedures
- Procedures
- Automating DR/BC Documentation Process
- DR/BC Plan Sample Outline
- Up Front Information
- Chapter Review
- **Module 7 - Awareness and Training Programs**
- Awareness and Training Programs
- Elements of Awareness & Training Programs
- Audience Types
- Awareness
- Awareness Programs
- Training Programs
- Why Plan Exercises are Important
- Testing & Drills
- Testing Types
- Establishing Exercise Programs
- Review Various Types of Tests
- Plan Testing Guidelines
- Evaluation Exercises
- Audit your Plan

- Chapter Review
- **Module 8 - Maintenance Policies**
- Maintenance Policies
- Maintenance
- Maintenance & Schedule Budgets
- Software Tools for Maintenance
- Input Criteria for Plan Maintenance
- Plan Distribution & Security
- Chapter Review
- **Module 9 - Crisis Communications**
- Crisis Communications
- Escalation Procedures
- Escalation & Activation Procedures
- Disaster Declaration Procedures
- Public Relations/Spokesperson Role
- Typical Audiences
- Audience Messages
- Sources of Information
- Incident Command Centre (ICC)
- ICC Chain of Command
- ICC Organisation
- Be Prepared to Work with Public Authorities
- Executing the Plan
- Chapter Review
- **Module 10 - Cyber Attacks**
- Cyber Attacks
- Computer Crime & Cyberattacks
- Cyberattack Scenarios
- Northeast Cyberattack Scenario
- Economic Impact of Malicious Code Attacks
- Including Cyberattacks in Definitions of Terrorism
- Domestic and International Terrorism
- Department of Homeland Security Key Assets
- Cyberspace Security Strategies
- Expectations of Cyberattacks
- Information Warfare
- Considerations for Developing Information Warfare Procedures
- Protection Against Cyberattacks
- How Computer Systems are Attacked
- Types of Computer Attacks
- Developing Procedure in the wake of a Security Breach
- Procedures to Follow After an Attack
- Developing Procedures to Determine economic Losses
- Developing Procedures to Ease IT Recovery
- Types of Systems and Networks
- Recovery of Small Computer Systems

- Recovery of Large Computer Systems
- Network Recovery
- Establishing a Computer Incident Response Team
- Important Points
- Chapter Review
- **Module 11 – Pandemics**
- Pandemics
- Quick Facts
- Pandemics
- Planning Issues per Stage
- Stage 4 Communications
- HR Policies
- Stage 3 HR Travel Policies
- Stage 3 Government Relations
- Stage 3 Physical Resources
- Pandemics
- Chapter Review
- Course Closure