Certified Disaster Recovery Engineer (4 Days)

When a business is hit by a natural disaster, cyber crime or any other disruptive tragedy, how should it react? What if the office IT infrastructure is taken down? Will the business be able to continue operations? How much will it cost if the business is down during repairs?

The answer lies in the training of the Certified Disaster Recovery Engineer Cybersecurity Training Course. Disaster recovery and business continuity planning is the process of having a professional work with a business to prepare processes, policies and procedures to follow in the event of a disruption. The goal is to keep a businesses critical operations running, which today heavily relies on its IT infrastructure.

Students who take this Cybersecurity Training Course will be prepared to work with businesses to create and implement disaster recovery and business continuity plans.

Prerequisites

- CSS: Security Sentinel
- OR Equivalent Experience

Target Student:

The Certified Disaster Recovery Engineer Cybersecurity Training Course is designed for those understand business and its different processes, including the role that IT. We recommend those who take this Cybersecurity Training Course to have experience in risk, facilities, or security management. At the very least students should have equivalent experience and knowledge of what is covered in our C)SS: Security Sentinel Cybersecurity Training Course.

Cybersecurity Training Course Objective

Upon completion, students will:

- Understand the principles of business continuity and disaster recovery planning.
- Have a first draft of their own business continuity and disaster recovery plan.
- Be ready to sit for the CDRE certification exam.

Course Outline

Module 1 Welcome to Disaster Recovery Training

- mile2® Cybersecurity Training Course Road Map
- mile2® Brochure
- CDRE Agenda
- Schedule
- The CDRE Exam
- Introductions
- Introduction to Business Continuity Planning
- What is a Disaster?
- What is a Critical Business Function?
- Business Continuity Planning (BCP)
- Importance of BCP
- Disaster Recovery Planning (DRP)
- Emergency Response
- BC/DR Trends
- Purpose of BC/DR Program
- BCP Overview
- Challenges to Effective BCP

- BCP Planning Phases
- Where does Project Initiation fit into the Process?
- Project Initiation Phase
- BC/DR Program Life Cycle

Module 2 Business Impact Analysis

- BCP Planning Model
- BCP Planning Phases
- Where does BIA fit into the Process?
- What is a BIA?
- BIA Scope, Goal, and Objectives
- BIA Terminology
- Maximum Tolerable Downtime
- Recovery Point Objective
- Recovery Time Objective
- Recovery Time Examples
- BIA Process
- BIA Process- Disaster Mode Staffing
- BIA Process: Capacity & Performance Objectives
- BIA Tools
- Kick off Meeting
- Preparing for the BIA Interviews
- Conducting the Interviews
- BIA
- Notes on Data Collection
- Identify Dependencies
- Finalize Data Analysis
- BIA Report
- Presentation to Senior Management

Module 3 Risk Analysis

- BCP Planning Model
- BCP Planning Phases
- Where does the Risk Analysis fit into the Process?
- Functional Requirements
- Threats to Business Process
- Causes of Unplanned Downtime
- Risk Examples
- Risk Analysis Terminology
- Risk Analysis Activities
- Exposure Inventory
- Business Process Inventory
- Business Process Documentation
- Statement of Risk
- ALE Annualized Loss Expectancy
- Statement of Risk
- Risk Control Definition
- Identifying Existing Controls
- Physical Controls
- Risk Analysis
- Risk Assessment Report
- Compiling a Risk Assessment Report
- Risk Analysis Summary

Module 4 Design & Development Phase (BCP Strategies)

- BCP Planning Model
- BCP Planning Phases
- Where does BCP Strategies
- fit into the Process?
- Strategy Process
- BCP Strategies
- Summary
- BCP Planning Phases
- Where does BIA fit into the Process?
- Design & Development Phase
- BCP Design
- Emergency Response & Operations
- Emergency Response Components
- Develop ER Procedures
- ER Sources for Assistance
- BCP Design
- Alternate Recovery Site
- Selecting Vendors
- for DR/BC Services
- Site Recovery & Resumption
- Restoration of Primary Site
- Return to Primary Site
- Continuity Strategy: Insurance
- Evaluate Insurance Terms
- BCP Design

Module 5 IT Recovery Strategies

- BCP Planning Model
- BCP Planning Phases
- Where does IT Strategy fit into the Process?
- IT Recovery Strategy Process
- IT Recovery Strategies
- Examples of IT Recovery
- Tape Vault Facilities
- Disk Backups

- Replicated Disk Backups
- Deduplicated & Replicated Backups
- Backups: Replicated & Deduplicated
- Data Archiving
- Systems Replication
- Application Redundancy
- Telecommunications Strategies
- Alternate Recovery Sites
- Internal or Vendor BC/DR Services
- Selecting Vendors for BC/DR Services
- Evaluating Vendors of DR/BC Resources
- Critical Factors
- IT Recovery Strategies Assessment
- IT Recovery Strategies
- Summary
- BCP Planning Phases
- Where does IT Strategy fit into the Process?
- DR Plan Development
- DRP Design
- DR Plan Development
- DR Plan Design

Module 6 Implementation Phase

- BCP Planning Model
- BCP Planning Phases
- Where does BIA fit into the Process?
- Where does Implementation fit into the Process?
- Implementation of BCP
- Responsibility for BCP Implementation
- Determine Cost Estimates
- Management Approval and Funding
- Install & Configure
- Detailed Documentation
- Implement Operational Changes
- Procure Facilities & Services
- BCP Planning Phases
- Where does BIA fit into the Process?
- Awareness & Training
- Awareness Programs
- Training Programs

Module 7 Testing & Exercise

- BCP Planning Model
- BCP Planning Phases
- Where does Testing and Drills fit into the Process?
- Testing & Exercise Phase
- Testing & Drills
- Progression of Testing Types
- Testing Participants
- Test Script Example
- Testing Post-Mortem

Module 8 Maintaining & Updating

- BCP Planning Model
- BCP Planning Phases
- Where does Maintenance fit into the Process?
- Maintenance Policies and Procedures
- Plan Maintenance
- Maintenance & Schedule Budgets
- Software Tools for Maintenance
- Input Criteria for Plan Maintenance
- Plan Distribution & Security

Module 9 Execution Phase

- BCP Planning Model
- BCP Planning Phases
- Where does the Execution Phase fit into the Process?
- Execution Phase
- Escalation Procedures
- Disaster Declaration Procedures
- Public Relations/Spokesperson Role
- Typical Audiences
- Audience Messages
- Sources of Information
- Incident Command Centre (ICC)
- ICC Chain of Command
- ICC Organization
- Be Prepared to Work with Public Authorities
- Executing the Plan

Module 10 Cyber Attacks

- Computer Crime & Cyber Attacks
- Cyber Attack Scenarios
- Northeast Cyber Attack Scenario
- Economic Impact of Malicious Code Attacks
- Including Cyber Attacks in Definitions of Terrorism
- Domestic and International Terrorism
- Department of Homeland Security Key Assets
- Cyberspace Security Strategies

- Expectations of Cyber Attacks
- Cyber Attacks
- Information Warfare
- Considerations for Developing Information Warfare Procedures
- Protection Against Cyber Attacks
- Cyber Attacks
- Evolving Privacy Laws
- How Computer Systems are Attacked
- Types of Computer Attacks
- Developing Procedure in the wake of a Security Breach
- Cyber Attacks
- Developing Procedures for Working with Law Enforcement
- Cyber Attacks
- Developing Procedures to Determine Economic Losses
- Cyber Attacks
- 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
- Cyber Attacks
- Important Points

Module 11 – Pandemics

- What is Pandemic Influenza?
- Pandemics Quick Facts
- Why use BCP/DRP for Pandemic Influenza?
- Planning Approach
- Critical Services
- Additional Impacts of Pandemic
- Areas to Plan for
- Pandemics
- Planning Issues per Stage
- Stage 4 Communications
- HR Policies
- Stage 3 HR Travel Policies
- Stage 3 Government Relations
- Stage 3 Physical Resources
- Stage 3 & 4 Physical Resources
- Pandemics: Work from Home