5 Days

Disaster Recovery and Business Continuity

A disaster recovery plan (DRP) - sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) - describes how an organization is to deal with potential disasters. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions.

Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention. Disaster recovery is becoming an increasingly important aspect of enterprise computing. As devices, systems, and networks become ever more complex, there are simply more things that can go wrong. As a consequence, recovery plans have also become more complex.

According to Jon William Toigo (the author of Disaster Recovery Planning), fifteen years ago a disaster recovery plan might consist of powering down a mainframe and other computers in advance of a threat (such as a fire, for example, or the sprinkler system), disassembling components, and subsequently drying circuit boards in the parking lot with a hair dryer. Current enterprise systems tend to be too complicated for such simple and handson approaches, however, and interruption of service or loss of data can have serious financial impact, whether directly or through loss of customer confidence.

Appropriate plans vary a great from one enterprise to another, depending on variables such as the type of business, the processes involved, and the level of security needed. Disaster recovery planning may be developed within an organization or purchased as a software application or a service. It is not unusual for an enterprise to spend 25% of its information technology budget on disaster recovery. Six years after the events of 9/11, many corporate IT operations are overconfident about their ability to handle a disaster, according to a Forrester Research, Inc. 2007 report The survey of 189 data center decision makers found a severe lack of IT preparation for natural and manmade disasters. For example, the report found that 27% of the respondents

Course Details

Course Outline

Module 01: Introduction to Disaster Recovery and Business Continuity Disaster Recovery & Business Continuity:

- Terminologies Disaster Types Consequences of Disaster Disaster Recovery & Business Continuity
- Principles of Disaster Recovery and Business Continuity
- Disaster Recovery & Business Continuity: Issues Addressed Activities of Disaster Recovery & Business Continuity
- Disaster Recovery and Business Continuity Program Disaster Recovery & Business Continuity Solutions
- Best Practices in Disaster Recovery & Business Continuity Program
- International Strategy for Disaster Reduction (ISDR)

Module 02: Nature and Causes of Disasters:

- Nature of Disasters Categorization of Disasters
- Natural Disasters
- Earthquakes
- Protecting Yourself During Earthquake
- Volcanoes
- Protection from Volcanoes
- Forecasting Volcanoes

- Estimating Earthquakes
- Tsunami
- Protecting Yourself During Tsunami
- Landslides
- Effects of Landslides
- Protecting Yourself from Landslides
- Hurricanes
- Safety Measures During Hurricanes
- Predicting Hurricanes
- Floods
- Effect of floods
- Prevention
- Measures
- Wildfires
- Safety Measures
- Drought
- Consequences of Drought
- Measures to Overcome Drought Effects
- Man-Made Disasters Accidents
- Power Outage
- Telecommunication Outage
- Categorization of Human Intentional Disasters Arson Civil Disorder
- Terrorism War Page
- Chemical Biological Radiological Nuclear (CBRN)

Module 03: Emergency Management:

- Emergency
- Emergency Management
- Need for Emergency Management
- Emergency Management Phases
- Mitigation
- Preparedness
- Response Recovery
- Effect of Disaster on Business Organizations
- Emergency Management for Business Organizations
- FEMA- Federal Emergency Management Agency
- FEMA as an Organization Activities of FEMA

Module 04: Laws and Acts:

- Introduction
- Applicable Acts in DR Laws and Acts in United States of America
- Industries: Sarbanes-Oxley Act
- Foreign Corrupt Practices Act (FCPA)
- Healthcare: HIPAA Regulations
- Financial Institutions: Gramm-Leach-Bliley Act
- Flood Disaster Protection Act of 1973
- Robert T. Stafford Disaster Relief and Emergency Assistance Act CAN-SPAM Act of 2003
- Federal Financial Institutions Examinations Council (FFIEC)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Laws and Acts of Europe Data Protection Act 1998
- Transmission of Personal Data: Directive 2002/58/EC
- Personal Data: Directive 95/46/EC
- Insurance: Financial Groups Directive (FGD)
- The Foundation of Personal Data Security Law: OECD Principles
- Dutch Personal Data Protection Act
- Austrian Federal Act concerning the Protection of Personal Data
- German Federal Data Protection Act
- Laws and Acts in Australia
- Health Records and Information Privacy Act (HRIP)
- Financial Transactions Reporting (FTR) Act 1988

Module 05: Business Continuity:

- Management Business Continuity
- Management Business Continuity Planning
- Objectives of Business Continuity Planning
- Essential Resources in Business Continuity Planning

- Business Continuity Management
- Planning Steps
- ISO (International Organization for Standardization)
- Overview of BS 7799 / ISO 17799 ISO/IEC 17799:2005 ISO/IEC 17799:2005: Business Continuity Management
- Risk Analysis
- Risk Assessment
- Basic Elements of Risk Assessment
- Business Impact Analysis (BIA)
- Components of Business Impact Analysis
- Threat Analysis
- Risk Analysis and Business Impact Analysis
- Crisis Management
- Steps in Crisis Management
- Crisis Management Phases
- Compliance Preparedness
- Training and Resource Development
- Contingency
- Planning Points to remember in BCM Plan
- Testing Birmingham City Council

Who Should Attend

Network server administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals.

Pre Requisite

Pass exam 312-76 to achieve EC-Council Disaster Recovery Professional (EDRP) certification. Benefits EDRP is for experienced hands in the industry and is backed by a curriculum designed by the best in the field. Greater industry acceptance as seasoned security professional.

Exams

Disaster Recovery and Business Continuity [EDRP exam 312-76]

464, Udyog Vihar Phase
V,Gurgaon (Delhi
NCR)-122016,India

+91 8882 233 777

training@mercury.co.in

www.mercurysolutions.co

Date - May 24, 2025