

Certified Disaster Recovery Engineer

Modality: On Demand

Duration: 2 Hours

About this course:

This cyber security certification training series covers everything you need to know about becoming a certified disaster recovery engineer. Students will learn about business impact analysis, risk analysis, BDP strategies, IT recovery strategies, implementation phase, testing and exercise, maintenance and updating, execution phase, cyber attacks, and pandemics.

Being a Certified Disaster Recovery Engineer (CDRE) validates that you are prepared to work with businesses to create and implement disaster recovery and business continuity plans. Those who are certified will be working, as a professional, with a business to prepare processes, policies and procedures to follow in the event of a disruption. You are important to keep a businesses' critical operations running, which today heavily relies on its IT infrastructure.

The average salary for an IT Professional is **\$85,460** per year.

Course Objective:

- Introduction
- Business Impact Analysis
- Risk Analysis
- BDP Strategies
- IT Recovery Strategies
- Implementation Phase
- Testing and Exercise
- Maintenance and Updating
- Execution Phase
- Cyber Attacks
- Pandemics

Audience:

- IT Professional
- Chief Technology Officer
- System Administrator
- Disaster Recovery Professional
- Business Continuity Professional
- Risk Consultant.

Prerequisite:

- A minimum of 12 months experience in risk management, security or facilities management.

- Sound knowledge of business assessment and writing skills

Suggested prerequisite course:

[Assess and Plan for Risks - Risk Assessment Matrix](#)

Course Outline:

- Module 01 - Introduction
- Module 02 - Business Impact Analysis
- Module 03 - Risk Analysis
- Module 04 - BCP Strategies
- Module 05 - IT Recovery Strategies
- Module 06 - Implementation Phase
- Module 07 - Testing and Exercise
- Module 08 - Maintenance and Updating
- Module 09 - Execution Phase