

# **Risk Management Framework (RMF)**

**Modality: On Demand**

**Duration: 2.5 Hours**

## ***About this course***

This course gives you the most in-depth training in Risk Management Framework. This course has been designed in such an appropriate manner that it will cover all the important components and topics of Risk Management Framework for DoD Information Technology. RMF is a DoD procedure responsible for different cybersecurity issues. These include pinpointing the problem, assessing it, and then managing it. These are collectively called as management of cybersecurity potentiality and services. This is demonstrated in the form of various security controls, and warranting the operations of Information Systems (IS) and Platform Information Technology (PIT) systems. This course will give you a sound training in all these components.

## ***Learning Objectives:***

The course has the following learning objectives:

- Gaining a sound comprehension for the Risk Management Framework for DoD IT Authorization procedure.
- Gaining comprehension for FISMA and NIST procedures for warranting Federal IT systems.
- Describing the important functions and responsibilities of RMF for DoD IT.
- Describing the statutory and regulatory requirements.
- Adequate application of the learned skills in the realistic scenarios presented.

## **Course Outline:**

Chapter 1: Introduction

Chapter 2: Cybersecurity Policy Regulations and Framework

Chapter 3: RMF Roles and Responsibilities

Chapter 4: Risk Analysis Process

Chapter 5: Step 1 Categorize

Chapter 6: Step 2 Select

Chapter 7: Step 3 Implement

Chapter 8: Step 4 Assess

Chapter 9: Step 5 Authorize

Chapter 10: Step 6 Monitor