Cloud Security Manager

Class Code: CT-PCS01

The aim of this course is to explore relevant concepts related to security, risk, and compliance within the cloud computing environment. The objectives for this course are to enable you to apply the underpinning security concepts into an enterprise cloud computing environment. The risks and the impact of cloud computing must be understood in terms of both business and technical security challenges and their effect on business and technical governance and policy. The course also presents the terminologies used to describe security threats and issues and, in particular, those in cloud computing.

At the end of the course, you will be able to understand how to secure the different cloud computing services and deployment models and also how to design security in the cloud infrastructure, configurations, and applications running within a cloud computing environment. This course provides an overview of different security topics, such as identifying, categorizing, and protecting your assets within an enterprise cloud computing environment.

The course materials include comprehensive reference materials that help participants continue the educational experience after the course. This course helps prepare you for the Professional Cloud Security Manager (PCS) exam provided by the Cloud Credential Council. This course is endorsed, recognized, and supported by several key technology vendors and standards bodies. An exam voucher is included with this course.

What You'll Learn

- Security and governance concepts and challenges in cloud computing
- What is new in security in the cloud?
- Contract management, terms, and conditions and legal
- IaaS specific security and governance policies
- PaaS specific security and governance policies
- SaaS specific security and governance policies

Who Needs to Attend

- IT security professionals
- IT risk and compliance professionals
- Auditors of cloud computing services
- Network engineers/administrators and email system administrators

Prerequisites:

There are no formal prerequisites; however, it is recommended that participants have five years of Enterprise Security experience and solid understanding of cloud computing services and deployment models.

Cloud Security Manager

Class Code: CT-PCS01

Class Outline

1. Course Introduction:

- Overview
- Course Learning Objectives
- Course Agenda
- Case Study

2. Cloud Computing-Security, Governance, and Risks:

- Security, Governance, and Risks
- Cloud Computing Basics
- Cloud Computing Security

3. Security Threats and Challenges in Cloud Computing:

- Security and Compliance in Cloud
- Transparency, Accountability, and Viability
- Physical Security and Cloud Computing

4. Security Management in Cloud Computing:

- Identity and Access Management
- Data Classification
- Data Security Lifecycle

5. Legal, Contractual, and Operational Monitoring in Cloud:

- Legal and Regulatory Landscape
- Monitoring-Providers and Subscribers
- Security Operations in Cloud

6. Network Security Management in Cloud:

- Network Management in the Cloud
- Vulnerability, Patch Management, and Pen-Testing
- Cloud Security Architecture

7. Business Continuity, Disaster Recovery, and Capacity/Performance Planning:

- Business Continuity (BC)
- Disaster Recovery (DR) Resilient Technology
- Capacity and Performance Planning for Cloud

8. Advanced Cloud Security Management Practices:

- Container Cloud Security
- Secure Development Standards in Cloud
- Application Programming Interface API Security

9. Security Planning, Standards, and Cloud Evolution:

- Cloud Security Planning
- Cloud Standards, Controls, and Auditing
- Cloud Security Evolution

CierraTEC
training@cierratec.net
www.cierratec.net
(678) 389-4322