Certified Cloud Security Officer (CCSO)

Modality: On Demand

Duration: 21 Hours

About this Course:

The Cloud is being widely adopted today for a diverse set of reasons! However, many are finding that security in the cloud is a huge challenge! Either because of implementation or Governance. Yes, Governance of security related to your cloud vendor is a huge challenge. However, many global standards have been developed that provide a great baseline for cloud security along with governance. This course will provide for you what you do not find in other classes! The combination of knowledge combined into one source from the leading global standards. We also provide practical skills regarding implementing cloud security, auditing and compliance. This is all managed by a unique delivery of cloud security along with the hands-on labs needed to truly understand what is happening to your data at all the layers of the cloud stack.

Course Objectives:

- To fully understand Cloud Security from a real-world view point
- To receive the hands-on experience needed to implement Cloud Security with practical implementations
- To comprehend the industry security standards for both exam knowledge and implementation
- To have a general working knowledge on what to audit in a cloud architecture.
- To know hands-on methods of auditing a cloud environment from best practices view point.
- To understand how compliance is viewed and dealt with in the cloud.
- To gain the knowledge needed to pass the exam

Audience:

- Virtualization Administrators, Cloud Administrators, CIO, Virtualization and Cloud Auditors, Virtualization and Cloud Compliance Officers, anyone that needs a general understanding of security in the Cloud, those seeking the CCSP Certification.

Prerequisites:

- Recommended minimum one-year experience with virtualization technology or equivalent knowledge. General understanding of cloud architectures. Minimum one-year experience with general security.

Course Outline:

This Course Includes:

- Chapter 1 - Introduction to Cloud Computing and Architectural Concepts

- Chapter 2 - Cloud Risks
- Chapter 3 - ERM and Governance
- Chapter 4 - Legal Implications
- Chapter 5 - Virtualization and Technical Design
- Chapter 6 - Managing Information and Securing Data
- Chapter 7 - Data Center Operations
- Chapter 8 - Interoperability and Portability
- Chapter 9 - Traditional Security
- Chapter 10 - BCM and DR
- Chapter 11 - Incident Response
- Chapter 12 - Application Security
- Chapter 13 - Encryption and Key Management
- Chapter 14 - Identity, Entitlement and Access Management
- Chapter 15 - Auditing and Compliance