Certified Cloud Security Officer (C)CSO)

Modality: Virtual Classroom

Duration: 5 Days

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. This is a relevant course which introduces many technologies used in the cloud from implementing a private cloud architecture to using a new key management solution from various vendors.

Course Objective:

- 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.

Prerequisite:

- 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:

Module 1 – Introduction to Cloud Computing and Architecture

- Cloud Computing Terminology
- Cloud Computing Definition
- Cloud Computing Characteristics
- Cloud Computing Benefits

Module 2 – Cloud Risks

- Cloud Migration Security Evaluation
- ENISA Risk Evaluation

Module 3 – ERM and Governance

- Application of Governance and Risk
- Management to the Cloud

Module 4 – Legal Issues

- Understanding Unique Risks in the Cloud
- International Law and Potential Conflicts
- eDiscovery

Module 5 – Virtualization

- Virtualization Principles
- Key Components Mapped to Cloud Layer
- Key Security Concerns

Module 6 – Data Security

- Virtualization Principles
- Key Components Mapped to Cloud Layer
- Key Security Concerns

Module 7 – Data Center Operations

- Build Logical Infrastructure for Cloud Environment
- Manage Logical Infrastructure for Cloud Environment

Module 8 – Interoperability and Portability

- Interoperability
- Portability

Module 9 – Traditional Security

- The Physical Environment
- Support the Planning Process for the Data Center Design
- Implement and Build Physical Infrastructure for Cloud Environment

https://www.quickstart.com/ Contact Us: (866) 991-3924