ecom infotech (i)ltd

Comprehensive Cloud Security Training

As more and more organizations are adopting the cloud, Cloud Security and Privacy issues are on the rise. With data moving to the cloud and stringent security and privacy issues such as HIPAA, GDPR and PCI, it is pertinent for organizations to meet compliance norms and protect its data.

The new norm is Hybrid Cloud for organizations. It's not about should we need to move to cloud or not, according to many independent research about 70% of the major organizations have either moved or moving to the cloud for its various benefits. Major organizations have started offering Cloud services such as Amazon, Microsoft, Oracle, HP, Google, and other data center providers in various flavors such as Iaas, PaaS, SaaS, DRaaS etc. With IoT/IIoT data moving to the cloud for use of Analytics and AI, and Smart Infrastructure programs being implemented, data breaches are likely to be on the rise.

In our opinion there are not enough courses in today's market to cater to the various cloud challenges. Hence, we have designed a course with a holistic approach to look at the Certification requirements to individuals as well as to make sure there is a practical approach to solve day to day Cloud Security challenges with cloud environments such as Amazon AWS.

Our team is led by Mr. Ashwin Chaudhary, who is already certified in cloud environment as CCSK by Cloud Security Alliance (CSA). Besides he is also a CISSP, CISA, CISM, CRISC, CGEIT, ISO27001LA, ITIL, PMP certified along with his CPA and MBA qualifications. He has about 14 years of Cyber Security global experience out of his 30 years of industry experience.

Ecom Infotech I Ltd is an Amazon AWS Business Partner and an HPE Security Business Partner, under is arm of Cyber Shield Institute (CSI) is offering you this unique program to prepare yourself and your organization for the Cloud Security and Privacy challenges.

Our Cloud Security program is designed in 2 phases:

Phase I (CCSK) training program for Individuals interested in pursuing CSA's CCSK Certification.

CCSK™
Certificate of
Cloud Security Knowledge

About CCSK

"As enterprises move toward cloud computing, they are desperately seeking guidance and education in this new domain. CSA is bridging this gap and the CCSK provides an important first step in establishing baseline knowledge for individuals tasked with building and managing applications to the cloud."

~ Michael Sutton, CISO, Zscaler

Level 3 Neo Vikram, New Link Road, Andheri - West, Mumbai 400 058
Tel: 98694-36685 Email: info@ecominfotech.biz Web: **www.ecominfotech.biz**
CIN L32000MH1983PLC030400

ecom infotech (i)ltd

"This is the mother of all cloud computing security certifications. The Certificate of Cloud Security Knowledge certification is vendor-neutral, and certifies competency in key cloud security areas."

~ CIO.com, Top Ten Cloud Computing Certifications

About CSA

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

Day 1

Domain 1 Architecture

- NIST Definition of Cloud Computing (Essential Characteristics, Cloud Service Models, Cloud Deployment Models)
- Multi-Tenancy
- CSA Cloud Reference Model
- Jericho Cloud Cube Model
- Cloud Security Reference Model
- Cloud Service Brokers
- Service Level Agreements

Domain 2: Governance and Enterprise Risk Management

- Contractual Security Requirements
- Enterprise and Information Risk Management
- Third Party Management Recommendations
- Supply chain examination
- Use of Cost Savings for Cloud

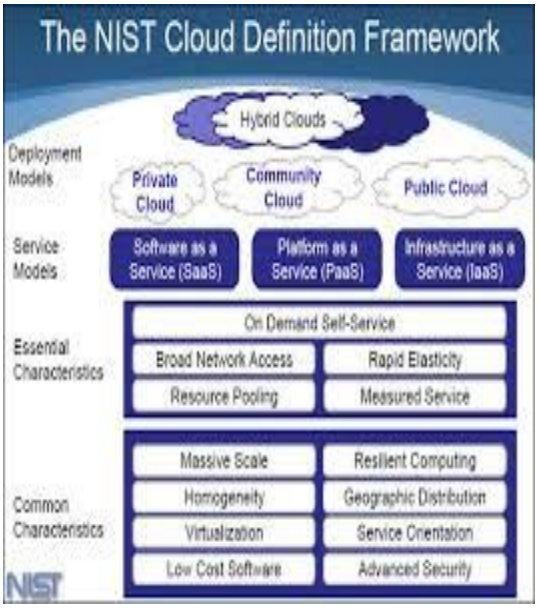
Domain 3: Legal Issues: Contracts and Electronic Discovery

- Consideration of cloud-related issues in three dimensions
- eDiscovery considerations
- Jurisdictions and data locations
- Liability for activities of subcontractors
- Due diligence responsibility
- Federal Rules of Civil Procedure and electronically stored information
- Metadata
- Litigation hold

Domain 4: Compliance and Audit Management

- Definition of Compliance
- Right to audit
- Compliance impact on cloud contracts
- Audit scope and compliance scope

- Compliance analysis requirements
- Auditor requirements



Day 2

Domain 5: Information Management and Data Security

- Six phases of the Data Security Lifecycle and their key elements
- Volume storage
- Object storage
- Logical vs physical locations of data
- Three valid options for protecting data
- Data Loss Prevention
- Detection Data Migration to the Cloud
- Encryption in IaaS, PaaS & SaaS
- Database Activity Monitoring and File Activity Monitoring
- Data Backup
- Data Dispersion
- Data Fragmentation

Domain 6: Interoperability and Portability

- Definitions of Portability and Interoperability
- Virtualization impacts on Portability and Interoperability
- SAML and WS-Security
- Size of Data Sets
- Lock-In considerations by IaaS, PaaS & SaaS delivery models
- Mitigating hardware compatibility issues

Domain 7: Traditional Security, Business Continuity, and Disaster Recovery

- Four D's of perimeter security
- Cloud backup and disaster recovery services
- Customer due diligence related to BCM/DR
- Business Continuity Management/Disaster Recovery due diligence
- Restoration Plan
- Physical location of cloud provider

Domain 8: Data Center Operations

- Relation to Cloud Controls Matrix
- Queries run by data center operators
- Technical aspects of a Provider's data center operations customer should understand
- Logging and report generation in multi-site clouds

Domain 9: Incident Response

- Factor allowing for more efficient and effective containment and recovery in a cloud
- Main data source for detection and analysis of an incident
- Investigating and containing an incident in an Infrastructure as a Service environment
- Reducing the occurrence of application level incidents
- How often should incident response testing occur

- Offline analysis of potential incidents

Day 3

Domain 10: Application Security

- Identity, entitlement, and access management (IdEA)
- SDLC impact and implications
- Differences in S-P-I models
- Consideration when performing a remote vulnerability test of a cloud-based application
- Categories of security monitoring for applications
- Entitlement matrix

Domain 11: Encryption and Key Management

- Adequate encryption protection of data in the cloud
- Key management best practices, location of keys, keys per user
- Relationship to tokenization, masking, anonymization and cloud database controls

Domain 12: Identity, Entitlement, and Access Management

- Relationship between identities and attributes
- Identity Federation
- Relationship between Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
- SAML and WS-Federation
- Provisioning and authoritative sources

Domain 13: Virtualization

- Security concerns for hypervisor architecture
- VM guest hardening, blind spots, VM Sprawl, data comingling, instant-on gaps
- In-Motion VM characteristics that can create a serious complexity for audits
- How can virtual machine communications bypass network security controls
- VM attack surfaces
- Compartmentalization of VMs

Domain 14: Security as a Service

- 10 categories
- Barriers to developing full confidence in security as a service (SECaaS)
- When deploying Security as a Service in a highly-regulated industry or environment, what should both parties agree on in advance and include in the SLA
- Logging and reporting implications
- How can web security as a service be deployed
- What measures do Security as a Service providers take to earn the trust of their customers
- VM guest hardening, blind spots, VM Sprawl, data comingling, instant-on gaps
- In-Motion VM characteristics that can create a serious complexity for audits
- How can virtual machine communications bypass network security controls
- VM attack surfaces
- Compartmentalization of VMs

ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security

- Isolation failure
- Economic Denial of Service
- Licensing Risks
- VM hopping
- Five key legal issues common across all scenarios
- Top security risks in ENISA research
- OVF
- Underlying vulnerability in Loss of Governance
- User provisioning vulnerability
- Risk concerns of a cloud provider being acquired
- Security benefits of cloud
- Risks R.1 – R.35 and underlying vulnerabilities
- Data controller vs data processor definitions
- in Infrastructure as a Service (IaaS), who is responsible for guest systems monitoring

The CCSK examination costs US$345.00. This entitles you to attempt the test up to two times. This amount is directly payable by you to CSA.

Phase II Practical Cloud Security Controls

Day 4 Amazon AWS.

- Introduction to Amazon AWS Cloud Computing
- AWS Security Controls
- AWS Shared Security Responsibility
- Security Logging and Monitoring
- Identity and Access Management at AWS
- Data Encryption
- Network Security
- Incident Management for Cloud
- Auditing AWS
- Governance and Compliance

Day 5 Best Practices & Review

- Aligning your ISO 27001 for Cloud Security Management
- ISO 27017/ 18 for Cloud Controls
- Cloud CSA CCM 3.0.1 and Cloud STAR Program
- NIST and other standards
- IoT for Cloud
- Review
- Internal Test

Course Delivery:

a. Workshop in various cities in batches of 10 and above from Mon-Fri
b. CCSK only course can be delivered from Fri-Sun
c. For Middle East Customers Sun-Thurs or for CCSK only Thurs-Sat
d. Corporate presentations in your premises
e. WebEx/Online delivery for a minimum 5 persons at a time. Total 40 hours.

Course Fees: Please contact us on info@ecominfotech.biz