Professional Cloud Security Manager Certification

Syllabus

What is the CCC Professional Cloud Security Manager certification?

The CCC Professional Cloud Security Manager (PCS) certification explores core concepts related to security, risk and compliance within the cloud computing environment. The certification enables candidates to apply the underpinning security concepts to 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 certification also presents the terminology used to describe security threats and issues in cloud computing.

Who is this certification for?

- IT Security Professionals (ie. Security Engineers, Analysts and Architects)
- Risk and Compliance Professionals (ie. Risk Management, Audit and Compliance Managers)
- Auditors of Cloud Computing Services, Network Engineers/Administrators and Email System Administrators

Syllabus - Professional Cloud Security Manager Certification

Mod 1. Course Introduction Module 2. Cloud Computing: Security, Governance, and Risks

2.1 Cloud Computing Basics

- Cloud Computing Primer: What is the Cloud
- Characteristics of Cloud Computing
- Cloud Service Models

- Cloud Deployment Models
- Cloud Reference Models

2.2 Security, Governance, and Risks in IT

- Information Security: Definition
- The CIA Principle
- Security Management
- Assets, Threats, Vulnerability, and Risk
- Risk Assessment
- Risk Assessment Result Matrix
- Executive Risk Treatment and Remediation Plan: Example
- Security Assessment
- Security Management Lifecycle
- Return on (Security) Investment
- Return on Security Investment: Example
- Information Security Management System

2.3 IT Governance

- Governance: Definition
- Governance Structure
- IT Governance Practices and Standards

2.4 Cloud Computing Security

- Cloud Computing: Shared Security Responsibility
- Security Risk Elements by Service Models
- Risks to Consider in the Cloud
  CIA Within the Cloud
  Multi-Tenancy
  Security Risks Within Multi-Tenancy Design
  Cloud Risk Considerations

Cloud Computing Security Reference Architecture
- Consumer: Cloud Computing Security Reference Architecture
- Cloud Provider: Cloud Computing Security Reference Architecture

Module 3. Physical and Operations Security: A Shared Responsibility

3.1 Security and Compliance: A Shared Responsibility
- Shared Security in Layered Architecture
- Security is a Shared Responsibility
- Split or Dual Responsibility
- Cloud Security Reference Model
- Cloud Compliance Control Layers
- Compliance Controls
- Cloud Provider Security Benefits
- Cloud Subscriber Security Benefits
- Cloud Consumer: Security Review
- Service Level Agreements: Specification of Responsibilities
- Cloud Computing Model SLA
- Cloud Interconnection Security Agreement
- Common Cloud Computing Vendor Trust Currencies

3.2 Physical and Operations Security Considerations
- Shared Security in Layered Architecture
- Authentication and Authorization in the Cloud
- Accountability and Responsibility in Respect to Cloud Providers and Subscribers
- Considerations for Data Transfer
- Loss of Control on Data
- Data Protection Issues in the Cloud
- Data Security Lifecycle
- Data Locations, Transfer, and Access
- Considerations Across the Data Lifecycle
- Cloud Computing and Data Protection Laws
- Vendor Lock-In
- Information Security and Defense
- Defense in Depth Within the Cloud
- Network Considerations in Cloud Computing

3.3 Risk Management: A Shared Perspective

- Assets Management in a Cloud Environment Threat Model for Cloud Service Deployment

Threat Modeling in the Cloud
Cloud Service Providers: Addressing Security and Risks in the Cloud
Cloud Service Providers: Understanding the Risks and Rewards Cloud
Subscriber Risk Assessment: Evaluating the Risks and Rewards

- Cloud Risk Assessment
- Risk Acceptance and Risk Treatment Plan
- Risk Treatment Summary
- Cloud Vendor Management: Shared Security and Risks Assessments

Module 4. Security Management Controls in Cloud Computing

4.1 Identity and Access Management

- Identity and Access Management: Definition
- Controlling Access
- Types of Security Credentials in the Cloud
- Federated Identity
- Multi-Factor Authentication
- MFA in the Cloud
- Identity Hub/Store
- Federated Identity Technologies
- Security Considerations in Using Federated Identity
- Least Privilege Access
- Role-Based Access (Security Groups) in the Cloud
- Sample Security Groups in the Cloud
- Separation of Duties

4.2 Data Protection

- Data Handling
- Data Protection: Primer
- Data Protection Requirements
- Data Security Standards
- International Data Protection Elements
- Data Governance
- Data Protection/Security Policy
- Data Classification: Overview
- Data Discovery Prior to Deploying to Cloud
- Data Classification Enablement
- Define Data Ownership
- Get the Users Involved: Start Classifying and Adding Metadata

4.3 Data Security Lifecycle

- Data Security

- Defining Principle: Data Geo-Location is Not a Security Principle
- Data Security Lifecycle Components
  Process Integration: Data Protection - in Transit
  Process Integration: Data Protection - At Rest and in Use
  Unstructured Data Protection
  Hardware Security Module
  HSM in the Cloud

4.4 Forensics in the Cloud

- Cloud Forensics
- Requirements for Forensics in the Cloud
- Forensics-Enabled Cloud

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

5.1 Legal and Regulatory Landscape

- Cloud Computing: Legal Challenges
- Legal and Regulatory Landscape: Cloud Computing
- Legal and Regulatory Landscape: Major Considerations
- Initial Due Diligence: Cloud Computing Contracting
- Cloud Computing Checklist
- Examples of Questions to be Asked
- Due Diligence: Common Trust Currencies
- Third-Party Involvement
- Cloud Computing Contracts
- Contracts in the Cloud: Data Protection
- Contracts in the Cloud: Scope of Processing

5.2 Monitoring: Providers and Subscribers

- Cloud Service Monitoring
- Cloud Computing Security Monitoring
- Cloud Continuous Monitoring
- Monitor Security and Performance of Applications
- Information Security Continuous Monitoring
- Interconnected Security Agreements

5.3 Security Operations in the Cloud

- Security Operations Center in the Cloud
- Security Operations: A Shared Responsibility
- Concept of Operations: Cloud Service Provider
- Example of Cloud Computing CONOPS: FedRAMP CONOPS
- Cloud Service and System Hardening
- Cloud Service Providers' Leading Practices: Hardening
- Cloud Service Subscribers' Leading Practices: Hardening

- TOP SLA Factors: Security Perspective

Module 6. Network Security Management in Cloud

6.1 Network Management in the Cloud

- Traditional Network Management vs. Cloud Network Management
- Cloud Computing Network Ecosystem
- Software-Defined Networking (SDN)

- SDN Security Considerations
- Network Service Virtualization (NSV)
- Virtualized Network: Security Challenges
- Security Advantages of Virtualization
- Virtual Infrastructure Security Secrets
- Role of Hypervisor
- Virtualization Security Challenges/Attack Vectors
- Cloud Network Security Management

6.2 Vulnerability, Patch Management, and Pen-Testing

- Vulnerability Management
- Vulnerability Management in the Cloud
- Threat and Vulnerability Management Programs
- VM Platforms
- Understanding Cloud Computing Vulnerabilities
- Vulnerability
- Vulnerabilities and Cloud Risk
- Cloud Computing
- Cloud Computing Core-Technology Vulnerabilities
- Essential Cloud Characteristic Vulnerabilities
- Architectural Components and Vulnerabilities
- Penetration Testing

6.3 Cloud Security Architecture

- Cloud Security Reference Architecture
- Composite Cloud Ecosystem Security Architecture
- Service-oriented Modeling Practices

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

7.1 Business Continuity

- Business Continuity Considerations
- Rationale for Maintaining Business Continuity Management Plan
- Business Continuity Executions
- Business Impact Analysis (BIA)
- BIA Results
- Business Continuity in Cloud
- Creating a Business Continuity Plan in Cloud
- Pros of Cloud Business Continuity
- Cons of Cloud Business Continuity
- Why Cloud Computing for BC/DR

-

7.2 Disaster Recovery Resilient Technology

Disaster Recovery (DR)

- Recovery Time Objective and Recovery Point Objective
- RPO and RTO Illustration
- Goal of DR: Balancing Business Requirements and Cost
- Mean Time to Repair (MTTR) and Mean Time Between Failure (MTBF)
- Traditional DR Investment Practices
- Alternative Recovery Strategies
- Tiered Data Storage for DR
- Causes for Data Loss
- Disaster Recovery in the Cloud
- Cloud Data Storage
- Cloud DR Compared To Traditional DR Solutions

7.3 Capacity and Performance Planning for Cloud

- Performance and Scalability
- Cloud Computing Infrastructure Implementation
- Performance Testing
- Cloud Workloads
- Critical Success Factors for Workloads in Cloud
- Cloud Computing Capacity Planning

Module 8. Advanced Cloud Security Management Practices

8.1 Advanced Security Considerations

- Cloud Container Overview
- Containers and Virtualizations
- Container Exploits
- Container Security Options: Docker
- Big Data
- MapReduce (Big Data)
- Hadoop: Security Concerns
- Big Data Challenges Are the Same as Traditional Data
- Secure Application Programming Interface Development
- Model-App Services Governance
- API Management vs. SOA
- API Barriers to Adoption

8.2 Secure Development Standards in Cloud

- Impact of Cloud on the Software Development Lifecycle
- Phases of IT Service Movement to the Cloud

-
- Basic Cloud Service Deployment
- Software Security Assurance
- Security in the Development Cycle
  Security Modeling: The Process

8.3 Cloud Security Planning

- Security Challenges in the Cloud
- Impacts to Cloud Security
- Create a Cloud Security Profile
- Identify Vulnerabilities for Your Selected Services
- Mitigate Security Vulnerabilities
- Prioritizing Your Security Investment in the Cloud

PROFESSIONAL CLOUD SECURITY MANAGER

CLOUD CREDENTIAL COUNCIL

Exam Details

Professional Cloud Security Manager Certification Exam	
Exam Type	Scenario Based, Complex Multiple Choice
Nr of Questions	25
Duration	60 minutes
Additional Time Provisions	15 minutes additional time for candidates who speak English as a second language.
Prerequisite	There are no formal prerequisite for this course. However, it is recommended that participants have five years of Enterprise Security experience and solid understanding of cloud computing services and deployment models.
Supervised (Proctored)	Yes (Live/Web)
Open Book	No
Pass Score	65%
Delivery	Online

Cloud Credential Council

The Cloud Credential Council (CCC) is an international member-based organization mandated to drive cloud readiness through effective competence development. The CCC has established critical cloud certifications for key IT roles in order to cultivate cloud-ready IT professionals. The certification scheme was developed after several years research investment in over 20 roles led by industry experts in conjunction with the leading technology vendors in the cloud computing arena.