CLOUD CREDENTIAL COUNCIL

PROFESSIONAL CLOUD SECURITY MANAGER

SYLLABUS

Syllabus for the certification course Cloud Security Manager leading to the CCC Professional Cloud Security Manager certification

Last Update: 15 of June 2016

© 2016 Cloud Credential Council

CLOUD CREDENTIAL COUNCIL

PROFESSIONAL CLOUD SECURITY MANAGER

List of contributors

Lead Author

Kumail Morawala

Contributors & Reviewers (to date):

Cuneyt Karul
Bill Lipiczky

© 2016 Cloud Credential Council

© 2016 Cloud Credential Council

CLOUD CREDENTIAL COUNCIL

PROFESSIONAL CLOUD SECURITY MANAGER

1. 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 terminologies used to describe security threats and issues in cloud computing.

2. Who is this certification for?

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

3. The Role of the Professional Cloud Security Manager

The challenge for professionals in security and governance in IT is in understanding the risks, issues and trade-offs presented by cloud computing.
The emergence of cloud computing has changed both the location and the domain of control of information technology. As on-premise hardware/software along with personal or corporate data is moved off-premise to a cloud or within the premises as a private cloud, the result is a change in ownership and responsibility for the systems, data and services. Current security and legal threats are shifting and new potential threats are being created.
This syllabus is concerned with applying security and governance best practice to a cloud environment. It draws on security guidelines such as those of the Cloud Security Alliance (CSA) and examines the key security issues of cloud computing and what types of business,

© 2016 Cloud Credential Council

commercial and technical governance are needed when managing cloud computing security.

4. Syllabus – Core Skills

Module 1. Course Introduction

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

Module Objectives

Explain the basic concepts of cloud computing.
Describe and explain the underpinning security concepts of information security and CIA.
Describe the key areas of security management.
Explain the risks and the impacts of cloud computing in terms of both business and technical security challenges and their effect on business and technical governance and policy.
Explain and implement risk treatments and mitigations in the cloud.

Key Topics

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

- Security, Governance, and Risks in IT
    - Information Security: Definition
    - The CIA Principle
    - Security Management
    - Assets, Threats, Vulnerability, and Risk
    - Risk Assessment

© 2016 Cloud Credential Council

- 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

IT Governance

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

· 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

Module Objectives

· Explain and implement shared security and compliance model of the cloud.
Explain the security risks and considerations of the cloud operations.
Explain the control and management tools to handle risks in cloud operations.

Key Topics

· Security and Compliance: A Shared Responsibility

© 2016 Cloud Credential Council

- 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

· 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

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

© 2016 Cloud Credential Council

- 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

Module Objectives

Explain the benefits of Identity and Access Management (IAM) including process automation and streamlining user interactions and self-service capabilities.
Explain and implement identity and access management in the cloud.
Explain the importance of having/using an enterprise Identity and Access Management Program framework.
Explain the concept of data classification and its importance in the cloud.
Explain the risks and the impacts of data protections at use, rest, and in-transit.
Explain the kinds of security implementations used to secure data in the cloud.

Key Topics

· 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·

© 2016 Cloud Credential Council

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

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

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

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

Module Objectives

Explain the concepts of legal and regulatory landscape within the cloud.
Explain the legal challenges in the cloud.
Explain and implement mitigations related to the key legal elements in the cloud.

© 2016 Cloud Credential Council

Explain the risks and opportunities for monitoring services in the cloud.
Identify the terminologies used to describe security threats and issues, in particular those related to cloud computing.

Key Topics

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

· 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

· 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 the Cloud

© 2016 Cloud Credential Council

Module Objectives

Explain network security.
Explain vulnerability management and security architecture in light of the advent of cloud computing.
Apply the awareness of vulnerability management and security architecture to their respective cloud computing role.

Key Topics

· Network Management in the Cloud
- Traditional Network Management vs. Cloud Network Management
- Cloud Computing Network Ecosystem
- Key Attributes of Cloud Networking
- Software-Defined Networking
- SDN Security Considerations
- Network Service Virtualization
- Virtualized Network: Security Challenges
- Security Advantages of Virtualization
- Virtual Infrastructure Security Secrets
- Virtualization Security Challenges/Attack Vectors
- Cloud Network Security Management

-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

· Cloud Security Architecture
- Cloud Security Reference Architecture
- Composite Cloud Ecosystem Security Architecture

© 2016 Cloud Credential Council

- Service-Oriented Architecture
- Service-Oriented Modeling Practices

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

Module Objectives

Explain the concepts of business continuity and disaster recovery.
Explain challenges within business continuity/disaster recovery in a traditional sense.
Explain implementation capabilities within business continuity/disaster recovery in the cloud.
Explain the risks and opportunities for using cloud as a business continuity/disaster recovery solution.
Explain the concept of capacity and performance planning in the cloud.

Key Topics

· Business Continuity
- Business Continuity Considerations
- Rational for Maintaining Business Continuity Management Plan
- Business Continuity Executions
- Business Impact Analysis
- BIA Results
- Business Continuity in the Cloud
- Creating a Business Continuity Plan in Cloud
- Pros of Cloud Business Continuity
- Cons of Cloud Business Continuity
- Cloud Computing for Business Continuity/Disaster Recovery· Disaster Recovery

· Disaster Recovery Resilient Technology
- Disaster Recovery
- Recovery Time Objective and Recovery Point Objective
- RPO and RTO Illustration
- Goal of DR: Balancing Business Requirements and Cost
- Mean Time to Repair and Mean Time Between Failure
- Traditional DR Investment Practices

© 2016 Cloud Credential Council

- 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

- 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

Module Objectives

Explain security considerations for the use of containers, Application Programming Interfaces (APIs), and Big Data.

Apply the awareness of security and governance issues for the development standards in the cloud.

Plan for cloud security.

Key Topics

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
-

© 2016 Cloud Credential Council

- API Management vs. SOA
- API Barriers to Adoption

- Secure Development Standards in the 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

- 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

© 2016 Cloud Credential Council

5. Course and Exam Details

Course Details

Suggested delivery format is instructor-led classroom-based learning.
Suggested duration: 24 learning hours.

Exam Details

Aspect	Details
Exam Type (Open book/Closed book)	Closed book
Number of Questions	25
Duration	75 minutes
Provisions for additional time relating to language	15 minutes of additional time
Prerequisite	None. However, it is recommended to attain the Cloud Technology Associate certification.
Supervised (Proctored)	Webcam Proctored
Open Book	No
Pass Score	65%
Delivery	Online

© 2016 Cloud Credential Council