PROFESSIONAL
CLOUD
SECURITY MANAGER

Syllabus

Syllabus for the certification course Cloud Security and Governance leading to the CCC Professional Cloud Security & Governance certification

CLOUD
CREDENTIAL
COUNCIL

CCC
Cloud Computing
PROFESSIONAL CLOUD
SECURITY MANAGER
Certified by
EXIN

List of contributors

Lead Author:

Mark Skilton – Capgemini

Contributors & Reviewers:

Todd Cioffi Navis Learning

Kumail Morawala - Combustec,

Ajeet Bagga VCE

Vladimir Baranek – Deloitte

Al Dunn – NJVC

Peter HJ van Eijk – Digital Infrastructures

Kevin L. Jackson – NJVC Mari J. Spina, D.Sc. – NJVC Karl Childs – HP

Contents

1. Overall Purpose of the Syllabus

The purpose of this syllabus is to provide a clear statement of the knowledge and skills required for cloud security and governance. This syllabus informs courseware providers of the training content required for accreditation. Furthermore, it provides guidance to instructors on which areas must be emphasized to give candidates the best possible chance of exam success. Finally, the syllabus also provides candidates themselves with clarity on what they must do to pass the exam and achieve certification.

2. Structure of the Syllabus

The structure of this syllabus is layered as follows:

The security and governance function itself is briefly described in relation to the background context of cloud computing.

Each module has a clearly-stated purpose and introductory synopsis followed by key topics and the specific learning objectives that must be met in order to achieve the required standard.

The flow of the learning modules is designed to build both understanding of the topics and practice in applying that knowledge to managing security and governance in a cloud environment.

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 and software, and personal and corporate data are 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 CSA and examines the key security issues of cloud computing and what types of business, commercial and technical governance are needed when managing cloud computing security.

4. Syllabus – Core Skills

Module 1. Course Introduction

Module Purpose and Overview

- Explain what it takes to secure the different cloud computing services and deployment models.
- Explain design security regarding the cloud infrastructure, configurations, and applications running within a cloud computing environment.
- Explain, apply, and analyze how to manage access to cloud computing resources using accounts, users, and groups.
- Explain, apply, and analyze the ways of securing data, operating systems, and applications and overall infrastructure within the cloud.

Key Topics

- Course Agenda
- Case Study
- Activities
- Course Book
- Questions and Answers

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

Module Purpose and Overview

- Explain the concept of governance, risk, and compliance.
- Describe and explain the underpinning security concepts of CIA.
- Explain and implement risk treatments and mitigations in the cloud.
- 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.
- Identify the terminologies used to describe security threats and issues in respect to cloud computing in particular.

Key Topics

- Security, Governance, and Risks
  - Information Security—Definition
  - Governance—Definition
  - Governance Structure—Example
  - Risk Assessment
  - Risk and Assets
  - Threats, Vulnerability, and Risk
  - The CIA principle
  - Risk Management Lifecycle
  - Security Assessments and Rewards
  - Risk Assessment Result Matrix
  - Executive Risk Treatment and Remediation Plan—Example
  - Security—Return on Investment
  - Security Management
- Cloud Computing Basics
  - Cloud Computing Primer—What is Cloud?
  - Cloud Computing Primer
  - Characteristics of Cloud Computing
  - Cloud Service Models
  - Types of Cloud Deployment Models
  - Defining Cloud Assets
  - Asset Identification Mapping and Matching
  - Security Risks in the Cloud—A Shared Security Perspective
  - New Risks to Consider in Cloud
  - Security Risk Elements by Service Models
- Cloud Computing Security
  - Cloud Computing—Shared Security Responsibility
  - Security Is a Shared Responsibility
  - Data Security Lifecycle
  - Data Locations, Transfer, and Access
  - Cloud Reference Model
  - Cloud Security Reference Model
  - Confidentiality, Integrity, and Availability (CIA) Within the Cloud
  - Multi-Tenancy
  - Security Risks Within Multi-Tenancy Design

- Cloud Risk Considerations
- Cloud Computing Reference Model
- Cloud Computing Security Reference Architecture
- Consumer: Cloud Computing Security Reference Architecture
- Cloud Provider: Cloud Computing Security Reference Architecture
- Cloud Computing Standards

Module 3. Security Threats and Challenges in Cloud Computing

Module Purpose and Overview

- Understand and explain the differences between traditional GRC and Cloud GRC.
- Explain the differences between security and compliance in cloud.
- Explain and implement shared security and compliance model.
- 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.

Key Topics

- Security and Compliance in Cloud
  - Overview
  - Cloud Governance, Risk, and Compliance
  - Cloud Provider, Subscriber Security, and Compliance Responsibilities
  - Cloud Provider Security Benefits
  - Cloud Subscriber Security Benefits
- Transparency, Accountability, and Viability
  - Specific Cloud Service Models and Security Issues
  - Handling Risks for Service and Deployment Models
  - Threat Modeling
  - Assets and Secure Asset Management in a Cloud Environment
  - Protect Assets in a Cloud Environment
  - Accountable Versus Responsible in the Context of Cloud Computing
  - Accountability and Responsibility in Respect to Cloud Providers and Subscribers
  - Information Security and Defense
  - Defense in Depth Within Cloud—A New Approach
- Physical Security and Cloud Computing
  - Cloud Service Providers—Addressing Security and Risks in Cloud
  - Cloud Service Providers—Understanding the Risks and Rewards
  - Cloud Subscriber Risk Assessment—Evaluating the Risks And Rewards
  - Cloud Risk Assessment
  - Data Protection in Cloud
  - Data Protections Laws and Cloud Computing
  - Data Management and Regulatory
  - Data Classification—Moving to Cloud
  - Vendor—Lock-in
  - Cloud Computing Vendor—Lock-in
  - Service Level Agreements (SLAs)
  - Cloud Computing Model SLA
  - Cloud Interconnection Security Agreement (ISA)
  - Common Cloud Computing Vendor Trust Currencies
  - Cloud Vendor Management—Shared Assessments
  - Risk Acceptance and Risk Treatment Plan
  - Risk Treatment Summary
  - Data Center Security
  - Network Considerations in Cloud Computing
  - Secure Data Transfers

Module 4. Security Management in Cloud Computing

Module Purpose and Overview

- Explain the concept of data classification and its importance in cloud.
- Explain the importance of having/using an enterprise Identity and Access Management Program framework.
- Explain the underpinning access management.
- 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 risks and the impacts of data protections at use, rest, and in-transit.
- Explain the kinds of security implementations reused to secure data in cloud.

Key Topics

- Identity and Access Management
  - Incorporating Identity and Access Management in Cloud
  - Controlling Access
  - Types of Security Credentials in Cloud
  - Federated Identity
  - Authoritative Source—Identity Management
  - Federated Identity Technologies
  - Security Considerations in Using Federated Identity
  - Multi-Factor Authentication
  - Multi-Factor Authentication (MFA) in Cloud
  - Least Privilege Access
  - Role-Based Access (Security Groups) in Cloud
  - Sample Security Groups in Cloud
  - Separation of Duties
- Data Classification
  - Data Handling
  - Data Protection—Primer
  - Data Protection Requirements
  - 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
- Data Security Lifecycle
  - Data Security
  - Defining Principle—Data Geo-Location Is Not A Security Principle
  - Data Security Lifecycle
  - Process Integration—Data Protection—in Transit
  - Process Integration—Data Protection—At Rest and in Use
  - Unstructured Data Protection
  - Hardware Security Module (HSM)
  - HSM in Cloud

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

Module Purpose and Overview

- Explain the concepts of legal and regulatory landscape within cloud.
- Explain the legal challenges in cloud.
- Explain and implement mitigations related to the key legal elements in cloud.
- Explain the risks and opportunities for monitoring services in 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
  - Initial Due Diligence—Cloud Computing Contracting
  - Cloud Computing Checklist
  - Examples of Questions to Be Asked
  - Due Diligence—Common Trust Currencies
  - Third-Party Involvement
  - Contract Compliance Fundamentals
  - Cloud Computing Contracts
  - Data Protection—Contracts in Cloud
  - Forensics in Cloud
  - Requirements for Forensics in Cloud
  - Forensics-Enabled Cloud
  - Summary of the Section
- Monitoring—Providers and Subscribers
  - Cloud Computing Security Monitoring
  - Monitoring—Cloud Service
  - Monitor Security and Performance of Applications
  - Cloud Continuous Monitoring
  - Outlining a Continuous Monitoring Process
  - Interconnected Security Agreements (ISA)
- Security Operations in Cloud
  - Areas of Practice—Security Operations in Cloud
  - Security Operations Center (SOC)—In Cloud
  - Security Operations—A Shared Responsibility
  - Concept of Operations—Cloud Service Provider
  - Example of Cloud Computing CONOPS—FedRAMP CONOPS
  - Security Operations—Subscriber Responsibilities
  - Cloud Service and System Hardening
  - Cloud Service Providers' Leading Practices—Hardening
  - Cloud Service Subscribers' Leading Practices—Hardening

Module 6. Network Security Management in Cloud

Module Purpose and Overview

- 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 specific cloud computing role.

Key Topics

- Network Management in the Cloud
  - Traditional Network Management vs. Cloud Network Management
  - Cloud Computing Network Ecosystem
  - Software-Defined Networking (SDN)
  - Open Networking Foundation (ONF)
  - SDN Security Considerations
  - Network Service Virtualization (NSV)
  - Security Advantages of Virtualization
  - Virtual Infrastructure Security Secrets
  - Role of Hypervisor
  - Virtualization Security Challenges/Attack Vectors
  - Cloud Network Security Management
- Vulnerability, Patch Management, and Pen-Testing
  - Vulnerability Management
  - VM Platforms
  - Understanding Cloud Computing Vulnerabilities
  - Vulnerabilities and Cloud Risk
  - Cloud Computing Core-Technology Vulnerabilities
  - Architectural Components and Vulnerabilities
  - Penetration Testing
  - Cloud Network Security Management in Context of Vulnerabilities
- Cloud Security Architecture
  - Cloud Security Reference Architecture
  - Composite Cloud Ecosystem Security Architecture
  - Service-Oriented Modeling Practices
  - OpenStack
  - Google App Engine
  - Windows Azure Deployment Architecture
  - AWS Web Application Architecture

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

Module Purpose and Overview

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

Key Topics

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

- Disaster Recovery (DR) 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
- 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 Purpose and Overview

- Explain specific security and governance issues for the PaaS model.
- Apply the awareness of security and governance issues for the PaaS model to design and manage PaaS systems.

Key Topics

- Container Cloud Security
  - Basic Differences Between Virtualizations vs. Containers
  - Cloud Container Overview
  - Containers Used in Platform as a Service (PaaS)
  - Container Exploits
  - Current Container Security Options
  - Big Data
  - MapReduce (Big Data)
  - Hadoop—Security Concerns
  - Big Data Challenges Are the Same as Traditional Data
- 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
  - Threat Modeling
  - Defining the Threats in Cloud
  - Secure Asset Management—What is an “Asset” in the Cloud
  - Remember the “Shared Responsibility”
- Application Programming Interface API Security
  - Application Programming Interface API Secure Development
  - New Model-App Services Governance
  - API Management vs. SOA
  - API Barriers to Adoption
  - APIs and Code
  - Local Data Center API Use

- Virtual Private Cloud
- Hybrid Cloud API Model
- SaaS API Model

Module 9. Security Planning, Standards, and Cloud Evolution

Module Purpose and Overview

- Examine specific security process and issues for the software, application, and services operating in the cloud.
- Apply security process and issues related knowledge to design and manage software systems.
- Plan cloud security.
- Explain cloud standards, controls, and auditing.
- Explain cloud security evolution.

Key Topics

- Cloud Security Planning
  - Security Challenges in Cloud
  - Impacts to Cloud Security
  - Create a Cloud Security Profile
  - Security Operations—A Shared Responsibility
  - Security Operations—Subscriber Responsibilities
  - Identify Vulnerabilities for Your Selected Services
  - Mitigate Security Vulnerabilities
  - Prioritizing Your Security Investment in the Cloud
  - Secure Your Use of the Cloud
  - Cloud Service Subscribers—Leading Practices—Hardening
- Cloud Standards, Controls, and Auditing
  - Cloud Security Control Frameworks
  - Cloud Computing Third Party Trust Certification Examples
  - Security Using Cloud
  - Security Compliance Responsibilities
  - Cloud Provider Security Benefits
  - Cloud Subscriber Compliance Benefits
  - Protect Assets in the Cloud
  - Cloud Service Providers—Understanding the Risks and Rewards
  - Defining Principle—Data Geo-Location Is Not Security Principle
  - Unstructured Data Protection
- Cloud Security Evolution
  - Cloud Provider, Subscriber Security, and Compliance Responsibilities
  - Federated Identity Evolution
  - Defense in Depth Within the Cloud—Review
  - Continuous Monitoring Process

5. Course & Exam Details

Course Details

Suggested delivery format is instructor-led classroom-based learning.

Suggested duration: 24 learning hours.

Exam Details

Aspect	Details
Exam Type	Online
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