



# Professional Cloud Security Manager

Duration 3 Days



PROFESSIONAL  
CLOUD  
SECURITY MANAGER

## COURSE DESCRIPTION

The Professional Cloud Security Manager (PCS) course is to explore relevant concepts related to security, risk and compliance within the cloud computing environment. The objectives for this course are to enable the candidates to apply the underpinning security concepts into 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 course also presents the terminologies used to describe security threats and issues and, in particular, those in cloud computing.

At the end of the course, the learner will be able to understand how to secure the different cloud computing services and deployment models and also how to design security in the cloud infrastructure, configurations and applications running within a cloud computing environment. It helps in understanding, applying and analyzing how to manage access to cloud computing resources using accounts, users and groups; and ways that the security manager can secure the data, operating systems, and applications and overall infrastructure within the cloud.

The course materials include comprehensive reference materials that help participants continue the educational experience after the course. The course prepares candidates for the Professional Cloud Security Manager exam provided by the Cloud Credential Council.

## AUDIENCE

The Professional Cloud Security Manager course will be of interest to:

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

## LEARNING OBJECTIVES

By the end of this course participants gain competencies in, and are able to:

- 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 methods to secure data, operating systems, applications, and the overall infrastructure of the cloud.

## PREREQUISITES

There are no formal prerequisites; however, it is recommended that participants have five years of Enterprise Security experience and solid understanding of cloud computing services and deployment models.



## COURSE OUTLINE

### Module 1: Course Introduction

- Overview
- Course Learning Objectives
- Course Agenda
- Activities
- Case Study
- Certification

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

- Module Learning Objectives
- Module Topics
- Cloud Computing Basics
- Information Security Management
- IT Governance
- Cloud Computing Security
- Module Summary

### Module 3: Physical and Operations Security: A Shared Responsibility

- Module Learning Objectives
- Module Topics
- Security and Compliance: A Shared Responsibility
- Physical and Operations Security Considerations
- Risk Management: A Shared Perspective
- Module Summary

### Module 4: Security Management Controls in Cloud Computing

- Module Learning Objectives
- Module Topics
- Identity and Access Management
- Data Protection
- Data Security Lifecycle
- Forensics in the Cloud
- Module Summary
- Summary

### Module 5: Legal, Contractual, and Operational Monitoring in the Cloud

- Module Learning Objectives
- Module Topics
- Legal and Regulatory Landscape
- Monitoring: Providers and Subscribers
- Security Operations in the Cloud
- Module Summary

### Module 6: Network Security Management in the Cloud

- Module Learning Objectives
- Module Topics
- Network Management in the Cloud
- Vulnerability Management
- Cloud Security Architecture
- Module Summary

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

- Module Learning Objectives
- Module Topics
- Business Continuity
- Disaster Recovery Resilient Technology
- Capacity and Performance Planning for Cloud
- Module Summary

### Module 8: Advanced Cloud Security Management Practices

- Module Learning Objectives
- Module Topics
- Advanced Security Considerations
- Secure Development Standards in the Cloud
- Cloud Security Planning
- Module

## ABOUT THE EXAM

- **Exam Format:** Closed Book
- **Question:** 25 questions
- **Pass score:** 65%
- **Duration:** 60 minutes. For non-native English speakers an additional 15 minutes is available.

## EXAM DESCRIPTION

The Professional Cloud Security Manager exam is delivered and evaluated by EXIN on behalf of CCC.