

## Description:

Mile2's Cloud Security Officer, C)CSO, course will provide you something you will not find in other class! The Cloud is being widely adopted today for a diverse set of reasons. However, many are finding that security in the cloud is a huge challenge.



The C)CSO looks to fill the gap in cloud security education and give you the skills you need to develop strong cloud security.

What makes this course powerful is the pairing of knowledge from leading cloud security authorities, with practical lab exercises. You will leave the course with a solid understanding of the cloud stack having been introduced to many technologies used in the cloud. Whether you are implementing private cloud architecture or managing solutions from various vendors, this course is for you.



Annual Salary Potential \$121,000 AVG/year

### Key Course Information

Live Class Duration: 5 Days

CEUs: 40

Language: English

Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

(Any of the following Mile2 Courses)

- 12 months experience with virtualization technology or equivalent knowledge.

- General understanding of cloud architectures

- Minimum 12 months experience with general security

### Modules/Lessons

Module 1 – Introduction to Cloud Computing and Architecture

Module 2 – Cloud Security Risks

Module 3 – ERM and Governance

Module 4 – Legal Issues

Module 5 – Virtualization

Module 6 – Data Security

Module 7 – Data Center Operations

Module 8 – Interoperability and Portability

Module 9 – Traditional Security

Module 10 – BCM and DR

Module 11 – Incident Response

Module 12 – Application Security

Module 13 – Encryption and Key Management

Module 14 – Identity, Entitlement and Access

Module 15 – Auditing and Compliance

### Labs

Lab 1 – Cloud Migration Evaluation

Lab 2 – Service Level Agreement Compliance

Lab 3 – Virtualization 101

Lab 4 – Understanding Network Traffic

Lab 5 – Hardening Your Virtual Machines

Lab 6 – ESXi Hosting Hardening

Lab 7 – Hardening vCenter

Lab 8 – Basics of Data Security in Azure

Lab 9 – 23: See Detailed Outline Below

\*All labs are performed in our Cyber Range® on our Ghost Pentesting Platform®



## Who Should Attend

- Virtualization Admins
- Cloud Security Officers
- CIO
- Virtualization and Cloud Auditors
- Virtualization and Cloud Compliance Officers

## Upon Completion

Upon completion, Certified Cloud Security Officer students will understand Cloud security from a real-world viewpoint and comprehend the industry security standards. The student will also be prepared to take the C)CSO exam.

## Accreditations



## Exam Information

The Certified Cloud Security Officer exam is taken online through Mile2's Learning Management System and is accessible on your Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

## Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

- 1) Pass the most current version of the exam for your respective existing certification
- 2) Earn and submit 20 CEUs per year in your Mile2 account.

## Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at [www.mile2.com](http://www.mile2.com).

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

## Course and Certification Learning Options



## Detailed Outline:

### Course Introduction

#### Module 1 – Introduction to Cloud Computing and Architecture

1. Cloud Computing Terminology
2. Cloud Computing Definition
3. Cloud Computing Characteristics
4. Cloud Computing Benefits
5. Cost Benefit Analysis Reference Model
6. What is Security for the Cloud?

#### Module 2 – Cloud Risks

1. Cloud Migration Security Evaluation
2. ENISA Risk Evaluation
3. Cloud Controls Matrix
4. Relevant CCM Controls

#### Module 3 – ERM and Governance

1. Application of Governance and Risk Management to the Cloud
2. Importance of the SLA
3. Relevant CCM controls

#### Module 4 – Legal Issues

1. Understanding Unique Risks in the Cloud International Law and Potential Conflicts eDiscovery
2. Contract Considerations
3. Relevant CCM Controls

#### Module 5 – Virtualization

1. Virtualization Principles
2. Key Components Mapped to Cloud Layer
3. Key Security Concerns
4. Other Technologies Used in the Cloud
5. The Layers
6. Relevant CCM Controls

#### Module 6 – Data Security

1. Cloud Data Life Cycle
2. Design and Implement Cloud Data Storage Architectures

3. Design and Apply Data Security Strategies Understand and Implement Data Discovery and Classification Technologies
4. Design and Implement Relevant Jurisdictional Data Protection for PII
5. Design and Implement Data Rights Management
6. Plan and Implement Data Retention, Deletion and Archival Policies
7. Design and Implement Auditability, Traceability, and Accountability of Data Events
8. Relevant CCM Controls

## Module 7 – Data Center Operations

1. Build Logical Infrastructure for Cloud Environment
2. Manage Logical Infrastructure for Cloud Environment
3. Manage Communications with Relevant Parties
4. Relevant CCM Controls

## Module 8 – Interoperability and Portability

1. Interoperability
2. Portability
3. Relevant CCM Controls

## Module 9 – Traditional Security

1. The Physical Environment
2. Support the Planning Process for the Data Center Design
3. Run Physical Infrastructure for Cloud Environment
4. Implement and Build Physical Infrastructure for Cloud Environment
5. Manage Physical Infrastructure for Cloud Environment
6. Relevant CCM Controls

## Module 10 – BCM and DR

1. Disaster Recovery and Business Continuity Management
2. Examples
3. Relevant CCM Controls

## Module 11 – Incident Response

1. Incident Response
2. Forensics
3. Relevant CCM Controls

## Module 12 – Application Security

1. Training and Awareness
2. Secure Software Development Life Cycle Process
3. Application of the Secure Software Development Life Cycle
4. Verifying the use of Secure Software
5. Identity and Access Management (IAM) Solutions
6. Additional components for the Cloud Software Assurance and Validation
7. Relevant CCM Controls

## Module 13 – Encryption and Key Management

1. Review from other chapters
2. Key Management in today's cloud services
3. Recommendations
4. Relevant CCM Controls

## Module 14 – Identity, Entitlement and Access Management

1. Introduction to Identity and Access Management Identities and Attributes
2. Architectures for Interfacing to Identity and Attribute Providers
3. The Identity Recommendations
4. Relevant CCM Controls

## Module 15 – Auditing and Compliance

1. Compliance and Audit Cloud Issues Assurance Frameworks
2. Auditing
3. Relevant CCM Controls

## Labs

Lab 1: Cloud Migration Evaluation

Lab 2: Service Level Agreement (SLA) Compliance Lab 3: Virtualization 101

Lab 4: Understanding Network Traffic

Lab 5: Hardening your Virtual Machines

Lab 6: ESXi Host Hardening

Lab 7: Hardening vCenter

Lab 8: Basics of Data Security in Azure

Lab 9: IaaS

Lab 10: Deploying a Cloud

Lab 11: Basic Data Center Operations in Azure Lab 12: Interoperability and Portability

Lab 13: Business Continuity in Azure

Lab 14: PaaS in Azure

Lab 15: Encryption in Azure

Lab 16: Identity and Access Management in Azure

Lab 17: SaaS

Lab 18: S-P-I Model Exercise

Lab 19: Cloud Business Driver Audit Exercise

Lab 20: IaaS Risk Assessment

Lab 21: Identity and Access Control Management in the Private Cloud Lab 22: VM Security Audit

Lab 23: Encryption/Key Management in SaaS