Certified Cloud Security

Master the Leadership and Technical Skills to Secure the Cloud

In today's rapidly evolving digital landscape, cloud adoption is no longer optional — it's mission-critical. But with great agility comes complex risk. The C)CSO course is your comprehensive path to mastering cloud security from both a strategic and technical perspective. Built around the core principles of NIST 800-145, CSA Guidance, and fully aligned with the (ISC)² CCSP and Mile2 C)CSO exam objectives, this course dives deep into:

- Cloud risk management, identity and access governance, and secure architecture design
- Threat modeling, DevSecOps, and cloud-native security tools across AWS, Azure, and GCP
- Legal and compliance issues across jurisdictions — from FedRAMP to GDPR
- Real-world case studies and interactive scenarios to build decision-making confidence

Whether you're leading security initiatives, preparing for certification, or securing complex multi-cloud environments, C)CSO empowers you to lead with clarity, design with confidence, and defend with precision.

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:

- 12 months experience with virtualization technology or equivalent knowledge.
- General understanding of cloud architectures
- Minimum 12 months experience with general security

Modules/Lessons

01: Cloud Computing

02: Fundamental Technologies

03: Enterprise Risk Mgmt

04: Cloud Risks

05: Design Fundamentals

06: Encryption Capabilities

07: Data Security / Classification

08: Identity, Entitlement, Access

09: Application Security

10: Cloud Security Operations

11: Business, Disaster, Incidents

12: Legal, Auditing, Compliance

(Full Outline Below)

Labs

01: Cloud Migration Evaluation

02: Azure Data Security

03: Saas

04: Azure Data Center Ops

05: Interoperability and Portability

06: Business Continuity in Azure

07: PaaS in Azure

08: Encryption in Azure

09: Log Analytics in Azure

10: Encryption/Key Mgmt in IaaS

*All labs are performed in our Cyber Range® on our Ghost Pen Testing Platform®

(Full Lab Outline Below)

Certified Cloud Security

Who Should Attend

The C)CSO course is designed for professionals responsible for planning, managing, auditing, or securing cloud environments; whether leading from the boardroom or building from the console. This course bridges the gap between executive oversight and hands-on implementation, making it ideal for both technical and non-technical roles.

- Security Managers and CISOs
- IT Directors and Architects
- Cloud Engineers and DevOps
- GRC Analysts and Compliance
- System Administrators
- Security Analysts
- Audit and Risk Professionals

Accreditations

CNSS
COMMITTEE ON NATIONAL SECURITY SYSTEMS
U.S. DEPARTMENT OF HOMELAND SECURITY
NICCS
National Initiative for Cybersecurity Careers and Studies
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

Exam Information

The Certified Cloud Security Officer exam is taken online through Mile2's Learning Management System and is accessible on you 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.

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

01. Cloud Computing and Architectural Concepts

- Cloud Computing Definitions and Characteristics
- Cloud Roles and Responsibilities
- Cloud Security Concepts
- Cloud Models and Reference Architecture
- Applicable Standards for Cloud Adoption
- Applicability to the Business

02. Fundamental Technologies to Cloud Computing

- Virtualization
- Storage Virtualization
- Network Virtualization
- Database
- Orchestration

03. Enterprise Risk Management and Governance

- Introduction to Enterprise Risk Management (ERM) & Governance
- Cloud Governance Frameworks
- Cloud Risk Management & Compliance
- Cloud Policy Development
- Contracts & Cloud Service Agreements
- Governance Best Practices & Implementation Strategies

04. Cloud Risks

- What is Cloud Risk?
- Core Categories of Cloud Risk
- Current Top Cloud Risks (CSA Top Threats 2024)
- Conducting a Cloud Risk Assessment
- Real-World Risk Assessment

05. Design Fundamentals

- Introduction to Cloud Design Principles
- Traditional Cloud Architectures
- Distributed & Modular Cloud Designs
- Serverless Architectures
- Containerized Architectures
- Edge and Fog Computing
- Hybrid and Multi-Cloud Architectures
- Identity-Driven and Zero Trust Architectures
- Design Patterns by Use Case

06. Encryption Capabilities and Key Management

- Strategic Importance of Encryption and Key Management
- Advanced Encryption and Key Management Concepts
- Data at Rest Encryption
- Data in Transit Encryption
- Data in Use & Confidential Computing
- Advanced Key Management in the Cloud
- Implementation Best Practices and Optimization
- Risks, Challenges, and Advanced Mitigation
- Regulatory Compliance and Governance
- Future Trends and Innovations

07. Data Security and Classification

- Data Lifecycle in the Cloud
- Cloud Data Security Architectures
- Data Discovery and Classification
- PII, PHI, and Sensitive Data Protection
- Information Rights Management and Policy Enforcement
- Data Retention, Deletion, and Archival
- Data Event Accountability and Auditability

08. **Identity, Entitlement and Access Management**

- Introduction to Cloud IAM and Entitlements
- Identity Types and Attributes in the Cloud
- Cloud IAM Models and Architectures
- Entitlement Management and Access Governance
- IAM Threats and Misconfiguration Risks
- Identity-Centric Security Controls and Monitoring
- IAM Strategy and Best Practices

09. **Application Security**

- Application Security in the Cloud
- Secure Software Development Lifecycle (Secure SDLC)
- Identity Integration for Applications
- Containers & Kubernetes Security
- Cloud Application Vulnerabilities, Threats, and Risks
- Application Security Controls and Validation
- Software Assurance and Supply Chain Security

10. **Cloud Security Operations Management**

- Operational Foundations in the Cloud
- Monitoring, Logging, and Observability in Cloud Environments
- Automation and Orchestration of Security Operations
- Security Communication and Collaboration
- AI/ML in Cloud Security Operations
- Metrics, Maturity, and Optimization of Cloud SecOps

11. **Business Continuity, Disaster Recovery and Incident Response**

- Foundations of BCDR and Incident Response
- Cloud-Specific BCDR Considerations
- Incident Response in Cloud Environments
- Resilience and Automation
- Testing, Drills, and Compliance Requirements
- Real-World Cloud Disruptions and Response Lessons

12. Legal, Auditing and Compliance Responsibilities

- Cloud-Specific Legal Considerations
- Global Cloud Laws and Regulations
- Contractual and SLA Considerations
- Compliance Frameworks and Industry Standards
- Auditing Cloud Environments
- Legal Incident Response and E-Discovery in the Cloud
- Emerging Legal Trends and Regulatory Horizon

Labs Outline:

Lab 01: Cloud Migration Evaluation

Lab 02: Service Level Agreement (SLA) Compliance Lab 3: Virtualization 101

Lab 04: Understanding Network Traffic

Lab 05: Hardening your Virtual Machines

Lab 06: ESXi Host Hardening

Lab 07: Hardening vCenter

Lab 08: Basics of Data Security in Azure

Lab 09: 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