Annual Salary Potential $89,862 AVG/year

Mile2's Certified Security Leadership Officer course is designed for mid and upper-level managers. If you are an engineer, this course will increase your knowledge in the leading information system security teams.

Icon

Description automatically generated



Description:

Plus, the C)SLO will give you an essential understanding of current security issues, best practices, and technology. With this knowledge you will then be prepared to manage the security component of an information technology project. As a Security Leadership Officer, you will be the bridge between cybersecurity and business operations.

\* This course/certification has been validated by the NSA for: CNSSl-4014, Information Assurance Training Standard for Information Systems Security Officers.

Who Should Attend



Key Course Information

**Live Class Duration:** 5 Days

**CEUs:** 32

**Language:** English

**Class Formats Available:**

Instructor Led

Self-Study

Live Virtual Training

**Suggested Prerequisites:**

\* 12 months professional experience

in IT

or

\* 12 months professional experience

in systems management

**Module 1** - Security Management

**Module 2** - Risk Management

**Module 3** - Encryption

**Module 4** - Information Security Access Control Concepts

**Module 5** - Incident Handling and Evidence Module 6 - Operations Security

**Module 7** - Network Security

Modules/Lessons

\* C - Level Managers

\* IT Managers

\* Cyber Security Personelle

\* Engineers

\* Information Systems

Owners

\* ISSO's

\* CISSP Students

\* ISO's

Accreditations

Logo

Description automatically generated





Key Course Information

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.

Upon completion, the Certified Security Leadership Officer candidate be able to competently take the C)SLO exam. You will be versed in implementing strong security controls and managing an organization with an industry acceptable security posture.

The Certified Security Leas 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.

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.

Upon Completion

Exam Information

Re-Certification Requirements

Course and Certification Learning Options



Graphical user interface, application

Description automatically generated



Detailed Outline:

**Module 1 - Security Management**

1. The Role of the CSLO
2. Business Goals and Objectives
3. Overview of Governance
   1. The First Priority for the CSLO
   2. Outcomes of Governance
   3. Performance and Governance
4. Organization of IT Security
5. Security Strategy
6. The Goal of Information Security
7. Defining Security Objectives
8. Security Budget
9. Security Integration
10. Architecture
11. Information Security Frameworks
12. Integration
13. COBIT 4.1
14. Deming and Quality
15. Ethics
16. Fraud
17. Hiring and Employment
18. Intellectual Property
19. Protecting IP
20. Attacks on IP
21. OECD Privacy Principles
22. PII and PHI
23. Awareness Training

**Module 2 - Risk Management**

1. Risk Management
2. Risk Assessment
3. Quantitative vs Qualitative Risk
4. What Is the Value of an Asset?
5. What Is a Threat/Vulnerability
6. Assess and Evaluate Risk
7. Controls
8. Comparing Cost and Benefit
9. Cost of a Countermeasure
10. Appropriate Controls
11. Documentation

**Module 3 – Encryption**

1. Encryption
2. Secrecy of the Key
3. Cryptographic Functions
4. XOR Function
5. Symmetric Encryption
6. Asymmetric Algorithms
7. Hashing Algorithms
8. Digital Signatures
9. Digital Envelope
10. Public Key Infrastructure (PKI)
11. Certificates
12. Uses of Encryption in Communications
13. Auditing Encryption Implementations
14. Steganography
15. Cryptographic Attacks

**Module 4 - Information Security Access Control Concepts**

1. Information Asset Classification
   1. Criticality
   2. Sensitivity
   3. Regulations and Legislation
2. Asset Valuation
3. Information Protection
4. Storing, Retrieving, Transporting and Disposing of Confidential Information
5. Password Policy
6. Password Cracking
7. Biometrics
8. Authorization
9. Accounting/Auditability
10. Centralized Administration
11. Access Control

**Module 5 - Incident Handling and Evidence**

1. Goals of Incident Management and Response
2. Security Incident Handling and Response
3. Evidence Handling
4. What is an Incident - Intentional
5. What is an Incident - Unintentional
6. Malware
7. Attack Vectors
8. Information Warfare
9. Developing Response and Recovery Plans
10. Incident Response Functions
11. Incident Management Technologies
12. Responsibilities of the CSLO
13. Crisis Communications
14. Challenges in Developing an Incident Management Plan
    1. When an Incident Occurs
    2. During an Incident
    3. Containment Strategies
    4. The Battle Box
    5. Evidence Identification and Preservation
    6. Post Event Reviews
15. Disaster Recovery Planning (DRP) and Business Recovery Processes
16. Development of BCP and DRP
17. Disaster Recovery Sites
18. Recovery of Communications
19. Plan Maintenance Activities
20. Techniques for Testing Security
21. Vulnerability Assessments
22. Penetration Testing

**Module 6 - Operations Security**

1. Operations Security
2. Specific Operations Tasks
3. Data Leakage – Object Reuse
4. Records Management
5. Change Control
6. Trusted Recovery
7. Redundant Array of Independent Disks (RAID)
8. Phases of Plan
9. BCP Risk Analysis
10. Recovery Point Objective
11. Priorities
12. OWASP Top Ten (2013)
13. Common Gateway Interface
14. How CGI Scripts Work
15. Cookies
16. Virtualization - Type 1
17. Virtualization – Type 2
18. Technologies – Databases and DBMS
19. Facilities
20. Facilities Security
21. Environmental Security
22. Physical Access Issues and Exposures
23. Controls for Environmental Exposures

Module 7 - Network Security

1. Network Topologies– Physical Layer
2. Data Encapsulation
3. Protocols at Each Layer
4. Devices Work at Different Layers
5. Technology-based Security
6. Network Security Architecture
7. Firewalls
8. Unified Threat Management (UTM)
9. UTM Product Criteria
10. TCP/IP Suite
11. Port and Protocol Relationship
12. Network Security
13. Internet Threats and Security
14. Auditing Network Infrastructure Security
15. IPSec - Network Layer Protection
16. Wireless Technologies– Access Point