CISSO
Certified Information System Security Officer

Overview
Mile2's Certified Information Systems Security Officer addresses the broad range of industry best practices, knowledge and skills expected of a security manager/officer. The candidate will learn in-depth theory pertaining to the practical implementation of core security concepts, practices, monitoring and compliance in the full panorama of IS management. Through the use of a risk-based approach, the CISSO is able to implement and maintain cost-effective security controls that are closely aligned with both business and industry standards. Whether you're responsible for the management of a Cyber Security team, a Security Officer, an IT auditor or a Business Analyst, the C)ISSO certification course is an ideal way to increase your knowledge, expertise, and skill.

Accreditation
ACCREDITED by the NSA CNSS 4011-4016
MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework
APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

Upon Completion
Upon completion, **Certified Information Systems Security Officer** students will not only be able to establish industry acceptable Cyber Security & IS management standards with current best practices but also be prepared to competently take the CISSO exam.

Course Length
5 days

Format
- Instructor-led classroom
- Computer Based Training
- Live Virtual Training

Prerequisites
- 1 Year experience in at least 2 modules or

- 1 year in IS Management

Student Materials

- Student Workbook
- Student Prep Guide

Certification Exam

- Mile2 C)ISSO – Certified Information Systems Security Officer
- Covers CISSP exam objectives

Who Should Attend?

- S Security Officers
- IS Managers
- Risk Managers
- Auditors
- Information Systems Owners
- IS Control Assessors
- System Managers
- Government

Course Contents

- **Module 1** - Risk Management
- **Module 2** – Security Management
- **Module 3** - Identification and Authentication
- **Module 4** - Access Control
- **Module 5** - Security Models and Evaluation Criteria
- **Module 6** - Operations Security
- **Module 7** - Vulnerability Assessments
- **Module 8** - Symmetric Cryptography and Hashing
- **Module 9** - Network Connections
- **Module 10** - Network Protocols and Devices
- **Module 11** - Telephony, VPNs, and Wireless
- **Module 12** - Security Architecture and Attacks
- **Module 13** - Software Development Security

- **Module 14** - Database Security and System Development
- **Module 15** - Malware and Software Attacks
- **Module 16** - Business Continuity
- **Module 17**- Disaster Recovery
- **Module 18** - Incident Management, Law, and Ethics
- **Module 19** - Physical Security