Certified Information Systems Security Officer

Course Duration: 5 Days, 40 Hrs

Course Overview

Mile2's vendor neutral Certified Information Systems Security Officer certification training was a direct initiative of the DND –Department of National Defence of Canada in cooperation with the DOD –Department of Defense of the United States; defined in the dual initiative titled CANUS CDISM MOU -ID#: 1974100118 found at: http://www.state.gov/documents/organization/111449.pdf. In the CANUS CDISM MOU, it stated the following:

- The CDRSN National Information System Security Officer (ISSO) is the focal point for all security issues pertaining to this network.
- The Director Information Management Security (DIMSECUR) is the DND authority for security assessment of the CDRSN, including the approval of Interim Authority to Process (IAP) and Authority to Communicate.

With these initiatives in mind, Mile2 created the Certified ISSO.

The CISSO addresses the broad range ofindustry 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.

Exam Information

The Certified Information Systems Security Officerexam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions

Course Content

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