Certified Information Systems Security Officer

KEY DATA

Course Name: Certified ISSO or C)ISSO

Duration: 5 days
Language: English

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 Exams:

- Mile2 C)ISSO – Certified Information Systems Security Officer
- Covers CISSP® 2015 exam objectives

CPEs: 40 Hours

WHO SHOULD ATTEND?
- IS Security Officers
- IS Managers
- Risk Managers
- Auditors
- Information Systems Owners
- IS Control Assessors
- System Managers
- Government

COURSE OVERVIEW

M2'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:

I.   The CDRSN National Information System Security Officer (ISSO) is the focal point for all security issues pertaining to this network.

II. 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 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.

Foundational Career

*

All combos Include:
- Online Video
- Electronic Book (Workbook/Lab guide*)

  *in all technical classes
- Exam Prep Questions
- Exam

ACCREDITATION

The **CISSO** certification has been validated by the **NSA** **CNSSI-4012, National Information Assurance** as well as the Training Standard for Senior System Managers and NSTISSI - 4011, National Training Standard for Information Systems Security (INFOSEC).

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.

EXAM INFORMATION

The **Certified Information Systems Security Officer** exam 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. The cost is $400 USD and must be purchased from Mile2.com.

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: Symmetric Cryptography and Hashing
Module 8: Asymmetric Cryptography and PKI
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

DETAILED MODULE DESCRIPTION

Module 1 - Risk Management
What Is the Value of an Asset?
What Is a ThreatSource/Agent?
What Is a Threat?
What Is a Vulnerability?
Examples of Some Vulnerabilities that Are Not Always Obvious
What Is a Control?
What Is Likelihood?
What Is Impact?
Control Effectiveness
Risk Management
Purpose of Risk Management
Risk Assessment
Why Is Risk Assessment Difficult?
Types of Risk Assessment
Different Approaches to Analysis
Quantitative Analysis
ALE Values Uses
Qualitative Analysis - Likelihood
Qualitative Analysis - Impact
Qualitative Analysis – Risk Level
Qualitative Analysis Steps
Management's Response to Identified Risks
Comparing Cost and Benefit
Cost of a Countermeasure

Module 2 - Security Management
Enterprise Security Program
Building A Foundation
Planning Horizon Components
Enterprise Security – The Business Requirements
Enterprise Security Program Components
Control Types
"Soft" Controls
Technical or Logical Controls
Physical Controls
Security Roadmap
Senior Management's Role in Security
Negligence and Liability
Security Roles and Responsibilities
Security Program Components
Security and the Human Factors
Employee Management
Human Resources Issues
Importance to Security?
Recruitment Issues
Termination of Employment

Informing Employees
About Security
Enforcement
Security Enforcement Issues

Module 3 - Authentication
Agenda
Access Control Methodology
Access Control Administration
Accountability and Access Control
Trusted Path
Who Are You?
Authentication Mechanisms
Strong Authentication
Authorization
Access Criteria
Fraud Controls
Access Control Mechanisms
Agenda
Biometrics Technology
Biometrics Enrollment Process
Downfalls to Biometric Use
Biometrics Error Types
Biometrics Diagram
Biometric System Types
Agenda
Passwords and PINs
Password "Shoulds"
Password Attacks
Countermeasures for Password Cracking
Cognitive Passwords
One-Time Password Authentication
Agenda
Synchronous Token
Asynchronous Token Device
Cryptographic Keys
Passphrase Authentication
Memory Cards
Smart Card
Agenda
Single Sign-on Technology
Different Technologies
Scripts as a Single Sign-on Technology
Directory Services as a Single Sign-on Technology
Thin Clients
Kerberos as a Single Sign-on Technology
Tickets
Kerberos Components Working Together

Major Components of Kerberos
Kerberos Authentication Steps
Why Go Through All of this Trouble?
Issues Pertaining to Kerberos
SESAME as a Single Sign-on Technology
Federated Authentication
Agenda
IDS
Network IDS Sensors
Types of IDSs
Behavior-Based IDS
IDS Response Mechanisms
IDS Issues
Trapping an Intruder

Module 4 - Access Control
Role of Access Control
Definitions
More Definitions
Layers of Access Control
Layers of Access Controls
Access Control Mechanism Examples
Access Control Characteristics
Preventive Control Types
Control Combinations
Administrative Controls
Controlling Access
Other Ways of Controlling Access
Technical Access Controls
Physical Access Controls
Accountability
Information Classification
Information Classification Criteria
Declassifying Information
Types of Classification Levels
Models for Access
Discretionary Access Control Model
Enforcing a DAC Policy
Mandatory Access Control Model
MAC Enforcement Mechanism – Labels
Where Are They Used?
Role-Based Access Control (RBAC)
Acquiring Rights and Permissions
Rule-Based Access Control
Access Control Matrix
Access Control Administration
Access Control Methods
Remote Centralized Administration
RADIUS Characteristics
RADIUS
TACACS+ Characteristics
Diameter Characteristics

Decentralized Access
Control Administration

Module 5 - Security Models and Evaluation Criteria
System Protection – Trusted Computing Base
System Protection– Reference Monitor
Security Kernel Requirements
Security Modes of Operation
System Protection– Levels of Trust
System Protection– Process Isolation
System Protection – Layering
System Protection - Application Program Interface
System Protection- Protection Rings
What Does It Mean to Be in a Specific Ring?
Security Models
State Machine
Information Flow
Bell-LaPadula
Rules of Bell-LaPadula
Biba
Clark-Wilson Model
Non-interference Model
Brewer and Nash – Chinese Wall
Take-Grant Model
Trusted Computer System Evaluation Criteria (TCSEC)
TCSEC Rating Breakdown
Evaluation Criteria - ITSEC
ITSEC Ratings
ITSEC – Good and Bad
Common Criteria
Common Criteria Components
First Set of Requirements
Second Set of Requirements
Package Ratings
Common Criteria Outline
Certification vs. Accreditation

Module 6 - Operations Security
Operations Issues
Role of Operations
Administrator Access
Computer Operations – Systems Administrators
Security Administrator
Operational Assurance
Audit and Compliance
Some Threats to Computer Operations
Specific Operations Tasks
Product Implementation Concerns
Logs and Monitoring
Records Management
Change Control
Resource Protection

Router
Gateway
Bastion Host
Firewalls
Firewall – First line of defense
Firewall Types – Packet Filtering
Firewall Types – Proxy Firewalls
Firewall Types – Circuit-Level Proxy Firewall
Type of Circuit- Level Proxy – SOCKS
Firewall Types – Application-Layer Proxy
Firewall Types – Stateful
Firewall Types – Dynamic Packet-Filtering
Firewall Types – Kernel Proxies
Firewall Placement
Firewall Architecture Types – Screened Host
Firewall Architecture Types – Multi- or Dual-Homed
Firewall Architecture Types – Screened Subnet
IDS – Second line of defense
IPS – Last line of defense?
HIPS
Unified Threat Management
UMT Product Criteria
Protocols
TCP/IP Suite
Port and Protocol
Relationship
Conceptual Use of Ports
UDP versus TCP
Protocols – ARP
Protocols – ICMP
Protocols – SNMP
Protocols – SMTP
Protocols – FTP, TFTP, Telnet
Protocols – RARP and BootP
Network Service – DNS
Network Service – NAT

Module 11 - Telephony, VPNs and Wireless
PSTN
Remote Access
Dial-Up Protocols and Authentication
 Protocols
Dial-Up Protocol – SLIP
Dial-Up Protocol – PPP
Authentication Protocols – PAP and CHAP
Authentication Protocol – EAP
Voice Over IP
Private Branch Exchange
PBX Vulnerabilities
PBX Best Practices
Virtual Private
Network Technologies
What Is a Tunnelling Protocol?

Tunnelling Protocols – PPTP
Tunnelling Protocols – L2TP
Tunnelling Protocols – IPSec
IPSec - Network Layer Protection
IPSec
IPSec
SSL/TLS
Wireless Technologies– Access Point
Standards Comparison
Wireless Network Topologies
Wi-Fi Network Types
Wireless Technologies – Access Point
Wireless Technologies – Service Set ID
Wireless Technologies – Authenticating to an AP
Wireless Technologies – WEP
WEP
Wireless Technologies –
More WEP Woes
Weak IV Packets
More WEP Weaknesses
How WPA Improves on WEP
How WPA Improves on WEP
TKIP
The WPA MIC Vulnerability
802.11i – WPA2
WPA and WPA2 Mode Types
WPA-PSK Encryption
Wireless Technologies – WAP
Wireless Technologies – WTLS
Wireless Technologies – Common Attacks
Wireless Technologies – War Driving
Kismet
Wireless Technologies – Countermeasures
Network Based Attacks
ARP Attack
DDoS Issues
Man-in-the Middle
Traceroute Operation

Module 12 - Security Architecture and Attacks
ESA Definition…
What is Architecture?
Architecture Components
Key Architecture Concepts - Plan
Objectives of Security Architecture
Technology Domain Modeling
Integrated Security is Designed Security
Security by Design
Architectural Models
Virtual Machines
Cloud Computing
Memory Types
Virtual Memory

Memory Management
Accessing Memory Securely
Different States that Processes Work In
System Functionality
Types of Compromises
Disclosing Data in an Unauthorized Manner
Circumventing Access Controls
Attacks
Attack Type – Race Condition
Attack Type - Data Validation
Attacking Through Applications
How Buffers and Stacks Are Supposed to Work
How a Buffer Overflow Works
Attack Characteristics
Attack Types
More Attacks
Host Name Resolution Attacks
More Attacks (2)
Watching Network Traffic
Traffic Analysis
Cell Phone Cloning
Illegal Activities

Module 13 - Software Development Security
How Did We Get Here?
Device vs. Software Security
Why Are We Not Improving at a Higher Rate?
Usual Trend of Dealing with Security
Where to Implement Security
The Objective
Security of Embedded Systems
Development Methodologies
Maturity Models
Security Issues
OWASP Top Ten (2011)
Modularity of Objects
Object-Oriented Programming Characteristic
Module Characteristics
Linking Through COM
Mobile Code with Active Content
World Wide Web OLE
ActiveX Security
Java and Applets
Common Gateway Interface
How CGI Scripts Work
Cookies
PCI Requirements
Virtualization - Type 1
Virtualization – Type 2

Module 14 - Database Security and System Development
Database Model

Database Models – Hierarchical
Database Models – Distributed
Database Models – Relational
Database Systems
Database Models – Relational Components
Foreign Key
Database Component
Database Security Mechanisms
Database Data Integrity Controls
Add-On Security
Database Security Issues
Controlling Access
Database Integrity
Data Warehousing
Data Mining
Artificial Intelligence
Expert System Components
Artificial Neural Networks
Software Development Models
Project Development – Phases III, IV, and V
Project Development–Phases VI and VII
Verification versus Validation
Evaluating the Resulting Product
Controlling How Changes Take Place
Change Control Process
Administrative Controls
Malware
Virus
More Malware
Rootkits and Backdoors
DDoS Attack Types
Escalation of Privilege
Protect against privilege escalation
DDoS Issues
DDoS
Buffer Overflow Definition
Overflow Illustration
Mail Bombing
E-Mail Links
Phishing
Spear Phishing
Replay Attack
Cross-Site Scripting Attack
Timing Attacks
More Advanced Attacks
Summary

Module 15 – Malware and Software Attacks
Malware
Virus
More Malware
Rootkits and Backdoors