

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® 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).



NICCS™

NATIONAL INITIATIVE FOR
CYBERSECURITY CAREERS AND STUDIES



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: Identity Management
- Module 4: Access Controls
- Module 5: Security Models
- 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
- Module 13: Software Development Security
- Module 14: Database Security
- Module 15: Malware and Software Attacks
- Module 16: Business Continuity
- Module 17: Incident Management
- Module 18: Physical Security

DETAILED MODULE DESCRIPTION

Module 1 - Risk Management

What Is the Value of an Asset?
 What Is a Threat Source/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 – Identity Management

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 Controls

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

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

Contingency Planning
System Controls
Trusted Recovery
 Fault-Tolerance Mechanisms
 Duplexing, Mirroring, Check Pointing
Redundant Array of Independent Disks (RAID)
Fault Tolerance
Redundancy Mechanism
Backups
Backup Types
Remote Access
Facsimile Security
Email Security
Before Carrying Out Vulnerability Testing
Vulnerability Assessments
Methodology
Penetration Testing
Penetration Testing
Hack and Attack Strategies
Protection Mechanism – Honeypot
Threats to Operations
Data Leakage – Social Engineering
Data Leakage – Object Reuse
Object Reuse
Why Not Just Delete File or Format the Disk?
Data Leakage – Keystroke Logging
Data Leakage – Emanation
Controlling Data Leakage – TEMPEST
Controlling Data Leakage – Control Zone
Controlling Data Leakage – White Noise
Summary

Module 7 - Symmetric Cryptography and Hashing

Cryptography Objectives
Cryptography Definitions
A Few More Definitions
Need Some More Definitions?
Symmetric Cryptography – Use of Secret Keys
Cryptography Uses Yesterday and Today
Historical Uses of Symmetric Cryptography
Historical Uses of Symmetric Cryptography – Scytale Cipher
Historical Uses of Symmetric Cryptography:
Substitution Cipher
Caesar Cipher Example
Historical Uses of Symmetric Cryptography: Vigenere Cipher
Polyalphabetic Substitution
Vigenere Table Example
Example Continued
Historical Uses of Symmetric Cryptography: Enigma Machine

Historical Uses of Symmetric Cryptography: Vernam Cipher
Historical Uses of Symmetric Cryptography: Running Key and Concealment
One-Time Pad Characteristics
Binary Mathematical Function
Key and Algorithm Relationship
Why Does a 128-Bit Key Provide More Protection than a 64-Bit Key?
Ways of Breaking Cryptosystems – Brute Force
Ways of Breaking Cryptosystems – Frequency Analysis
Determining Strength in a Cryptosystem
Characteristics of Strong Algorithms
Open or Closed More Secure?
Types of Ciphers Used Today
Encryption/Decryption Methods
Type of Symmetric Cipher – Block Cipher
S-Boxes Used in Block Ciphers
Type of Symmetric Cipher – Stream Cipher
Encryption Process
Symmetric Characteristics
Sender and Receiver Must Generate the Same Keystream
They both must have the same key and IV
Strength of a Stream Cipher
Let's Dive in Deeper
Symmetric Key Cryptography
Symmetric Key Management Issue
Symmetric Algorithm Examples
Symmetric Downfalls
Secret Versus Session Keys
Symmetric Ciphers We Will Dive Into
Symmetric Algorithms – DES
Evolution of DES
Block Cipher Modes – CBC
Different Modes of Block Ciphers – ECB
Block Cipher Modes – CFB and OFB
CFB and OFB Modes
Symmetric Cipher – AES
Other Symmetric Algorithms
Hashing Algorithms
Protecting the Integrity of Data
Data Integrity Mechanisms
Weakness in Using Only Hash Algorithms
More Protection in Data Integrity
MAC – Sender
MAC – Receiver
Security Issues in Hashing
Birthday Attack
Example of a Birthday Attack

Module 8 - Asymmetric Cryptography and PKI

Asymmetric Cryptography

Public Key Cryptography Advantages

Asymmetric Algorithm Disadvantages

Symmetric versus Asymmetric

Asymmetric

Asymmetric Algorithm – Diffie-Hellman

Asymmetric Algorithm – RSA

Asymmetric Algorithms – El Gamal and ECC

Example of Hybrid Cryptography

When to Use Which Key

Using the Algorithm Types Together

Digital Signatures

Digital Signature and MAC Comparison

What if You Need All of the Services?

U.S. Government Standard

Why Do We Need a PKI?

PKI and Its Components

CA and RA Roles

Let's Walk Through an Example

Digital Certificates

What Do You Do with a Certificate?

Components of PKI – Repository and CRLs

Steganography

Key Management

Link versus End-to-End Encryption

End-to-End Encryption

E-mail Standards

Encrypted message

Secure Protocols

SSL and the OSI Model

SSL Hybrid Encryption

SSL Connection Setup

Secure E-mail Standard

SSH Security Protocol

Network Layer Protection

IPSec Key Management

Key Issues Within IPSec

IPSec Handshaking Process

SAs in Use

IPSec Is a Suite of Protocols

IPSec Modes of Operation

IPsec Modes of Operation

Attacks on Cryptosystems

More Attacks

Module 9 - Network Connections

Network Topologies– Physical Layer

Topology Type – Bus

Topology Type – Ring

Topology Type – Star

Network Topologies – Mesh

Summary of Topologies

LAN Media Access Technologies

One Goal of Media Access Technologies

Transmission Types – Analog and Digital

Transmission Types – Synchronous and

Asynchronous

Transmission Types – Baseband and Broadband

Two Types of Carrier Sense Multiple Access

Transmission Types– Number of Receivers

Media Access Technologies - Ethernet

Media Access Technologies – Token Passing

Media Access Technologies – Polling

Cabling

Signal and Cable Issues

Cabling Types – Coaxial

Cabling Types – Twisted Pair

Types of Cabling – Fiber

Cabling Issues – Plenum-Rated

Types of Networks

Network Technologies

Network Technologies

Network Configurations

MAN Technologies – SONET

Wide Area Network Technologies

WAN Technologies Are Circuit or Packet Switched

WAN Technologies – ISDN

ISDN Service Types

WAN Technologies – DSL

WAN Technologies– Cable Modem

WAN Technologies– Packet Switched

WAN Technologies – X.25

WAN Technologies – Frame Relay

WAN Technologies – ATM

Multiplexing

Module 10 - Network Protocols and Devices

OSI Model

An Older Model

Data Encapsulation

OSI – Application Layer

OSI – Presentation Layer

OSI – Session Layer

Transport Layer

OSI – Network Layer

OSI – Data Link

OSI – Physical Layer

Protocols at Each Layer

Devices Work at Different Layers

Networking Devices

Repeater

Hub

Bridge

Switch

Virtual LAN

- 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

- 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

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
 DDoS Attack Types

Escalation of Privilege
DDoS Issues
DDoS

 Buffer Overflow Definition
 Overflow Illustration

 Buffer Overflows
Mail Bombing
E-Mail Links
Phishing
Spear Phishing
Replay Attack
Cross-Site Scripting Attack
Timing Attacks
More Advanced Attacks
Summary

Module 16 - Business Continuity

Phases of Plan
Who Is Ready?
Pieces of the BCP
BCP Development
Where Do We Start?
Why Is BCP a Hard Sell to Management?
Understanding the Organization
Critical products and services
Dependencies
Supply chain
Between departments
Personnel
Information
Equipment
Facilities
BCP Committee
BCP Risk Analysis
Identify Vulnerabilities and Threats
Categories
How to Identify the Most Critical Company Functions
Loss Criteria
Interdependencies
Identifying Functions' Resources
How Long Can the Company Be Without These Resources?
Calculating MTD
Recovery Point Objective
Calculation of maximum data loss
Determines backup strategy
Defines the most current state of data upon recovery
Recovery Strategies
Based on the results of the BIA
May be different for each department
Must be less than MTD
Sets the RTO
What Items Need to Be Considered in a Recovery?

Facility Backups – Hot Site
Facility Backups – Warm Site
Facility Backups – Cold Site
Compatibility Issues with Offsite Facility
Which Do We Use?
Choosing Offsite Services
Subscription Costs
Choosing Site Location
Other Offsite Approaches
BCP Plans Commonly and Quickly Become Out of Date
Summary

Module 17 - Incident Management

Seriousness of Computer Crimes
Incidents
Incident Management Priorities
Incident Response Capability
Incident Management Requires
Preparing for a Crime Before It Happens
Incident Response Phases
Types of Law
Foundational Concepts of Law
Common Laws – Criminal
Common Laws – Civil
Common Laws – Administrative
Intellectual Property Laws
More Intellectual Property Laws
Software Licensing
Digital Millennium Copyright Act
Historic Examples of Computer Crimes
Who Perpetrates These Crimes?
The Evolving Threat
Types of Motivation for Attacks
A Few Attack Types
Telephone Fraud
Identification Protection & Prosecution
Computer Crime and Its Barriers
Countries Working Together
Security Principles for International Use
Determine if a Crime Has Indeed Been Committed
When Should Law Enforcement Get Involved?
Citizen versus Law Enforcement Investigation
Investigation of Any Crime
Role of Evidence in a Trial
General Rules for Evidence
Evidence Requirements
Evidence Collection Topics
Chain of Custody
How Is Evidence Processed?
Evidence Types
Hearsay Rule Exception

Privacy of Sensitive Data
Privacy Issues – U.S. Laws as Examples
European Union Principles on Privacy
 Routing Data Through Different Countries
 Employee Privacy Issues

Computer Forensics
Trying to Trap the Bad Guy
Companies Can Be Found Liable
Sets of Ethics
Ethics – mile2
Ethics – Computer Ethics Institute
Ethics – Internet Architecture Board
GAISP- Generally Accepted Information Security
Principles

Module 18 - Physical Security

Physical Security – Threats
Different Types of Threats & Planning
Facility Site Selection
Facility Construction
Devices Will Fail
Controlling Access
Possible Threats
External Boundary Protection
Lock Types
Facility Access
Piggybacking
Securing Mobile Devices
Entrance Protection
Perimeter Protection – Fencing
Perimeter Protection – Lighting
Perimeter Security – Security Guards
Surveillance/Monitoring
Types of Physical IDS
Electro-Mechanical Sensors
Volumetric Sensors
Facility Attributes
Electrical Power
Problems with Steady Power Current
Power Interference
Power Preventive Measures
Environmental Considerations
Fire Prevention
Automatic Detector Mechanisms
Fire Detection
Fire Types
Suppression Methods
Fire Extinguishers