Certified Security Leadership Officer

KEY DATA

Course Name: Certified Security Leadership Officer

Duration: 5 days

Language: English

Format:

Instructor-led
Live Virtual Training

Prerequisites:

- A minimum of 12 months' professional experience in an IT or management

Student Materials:

- Student Workbook
- Student Prep Guide

CEU's: 40

WHO SHOULD ATTEND?

- C - Level Managers
- IT Managers
- Cyber Security Engineers
- Information Owners
- ISSO's
- CISSP students
- ISO's

COURSE OVERVIEW

The vendor neutral **Certified Security Leadership Officer**certification coursewas designed for mid and upper level managers as well as any engineers who seek to increase their knowledge in the security arena. The C)SLO coursewas designed to give management an essential understanding of current security issues, best practices, and technology. Because a security officer or manager understands the value of security, he or she is prepared to manage the security component of an information technology security projects.

A C)SLO candidate can be seen as the bridge between the cyber security team and operations as well as business management. Essentials topics covered in this management track are extremely detailed and include the following: Network Fundamentals and Applications, Hardware Architecture, Information Assurance Foundations, Computer Security Policies, Contingency and ContinuityPlanning, Business Impact Analysis, Incident Handling, Architect Approaches to Defense in Depth, Cyber Attacks, Vulnerability Assessment and Management, Security Policies, Web Security, Offensive and Defensive Information Warfare, culminating with Management Practicum.

IS Management Leadership

C)SS CERTIFIED SECURITY SENTINEL

C)ISSO Certified Information Systems Security Officer

IS 20 CONTROLS

C)SLO CERTIFIED SECURITY LEADERSHIP OFFICER *

All combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide)
- Exam Prep Questions
- Exam

ACCREDITATIONS

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

UPON COMPLETION

Upon completion, the **Certified Security Leadership Officer**candidate will not only be able to competently take the CSLO exam but will also be versed in implementing strong security controls and managing an organization with an industry acceptable security posture.

EXAM INFORMATION

The **Certified Security Leadership 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 DETAILS

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

C)SLO CERTIFIED SECURITY LEADERSHIP OFFICER

mile2 CYBER SECURITY CERTIFICATIONS

DETAILED MODULE DESCRIPTION

Module 1 - Security Management

The Role of the CSLO
Business Goals and Objectives
Vision
Overview of Governance
Importance of Information Security
The First Priority for the CSLO
Outcomes of Governance
Performance and Governance
Organization of IT Security
Developing a Security Strategy
Elements of a Strategy
Objectives of Security Strategy
The Goal of Information Security
Defining Security Objectives
Business Linkages
Business Case Development
Security Budget
Valuations
Security Program Priorities
What is Security?
Security Integration
Security Program
Architecture
Information Security Frameworks
Using a Framework
The Desired State of Security
Using the Balanced Scorecard
Align with Security Framework
ISO/IEC 27001 - The ISMS
Integration
Suitable for Organizations of all Sizes
COBIT 4.1
COBIT 4.1 Phases
Deming and Quality
Ethics
Fraud
Good to Great
Hiring and Employment
Employment
Culture
Marketing
Negotiating
Intellectual Property
Protecting IP
Attacks on IP
OECD Privacy Principles
PII and PHI
Awareness Training
Purpose of Awareness Training
Summary

Module 2 - Risk Management

Risk
Risk Management
Define a Risk Assessment Approach
Risk Factors
Enterprise Risk Management
Risk
Risk Assessment
Risk Analysis
Quantitative Risk
Qualitative Risk
What Is the Value of an Asset?
What Is a Threat Source/Agent?
What Is a Threat?
What Is a Vulnerability?
Assess and Evaluate Risk
Result of Risk Assessment
Inputs to Risk Treatment
Risk Definitions
Risk Treatment
Risk Acceptance
Definition of Controls
Control Types
“Soft” Controls
Technical or
Logical Controls
Physical Controls
Control Usage
Comparing Cost and Benefit
Cost of a Countermeasure
Appropriate Controls
Documentation
Statement of Applicability
Summary

Module 3 – Encryption

Encryption
Secrecy of the Key
Cryptographic Functions
XOR Function
Symmetric Encryption
Asymmetric Algorithms
Hashing Algorithms
Digital Signatures
Digital Envelope
Public Key Infrastructure (PKI)
Certificates
Uses of Encryption in Communications
Auditing Encryption Implementations
Steganography
Cryptographic Attacks
Summary

Module 4 - Information Security Access Control Concepts

Information Security Concepts (Agenda)
Information Asset Classification
Information Classification Considerations
Criticality
Sensitivity
Regulations and Legislation
Asset Valuation
Valuation Process
Information Protection
Storing, Retrieving, Transporting and Disposing of Confidential Information
Information Asset Protection
Access Control
Identification
Authentication
Password Policy
Password Cracking
Biometrics
Authorization
Authorization Best Practices
Accounting/Auditability
Trust Models
Centralized Administration
Discretionary Access Control
Mandatory Access Control
Role Based Access Control
Technologies – Access Control Lists
Summary

Module 5 - Incident Handling and Evidence

Definition
Goals of Incident Management and Response
History of Incidents
Security Incident Handling and Response
Evidence Handling
Best Evidence
What is an Incident - Intentional
What is an Incident - Unintentional
Malware
Attack Vectors
Information Warfare
Incident Management and Response
Developing Response and Recovery Plans
Incident Management and Response
Importance of Incident Management and Response
Incident Response Functions
Incident Management Technologies
Responsibilities of the CSLO
Crisis Communications
Challenges in Developing an Incident Management Plan
When an Incident Occurs
During an Incident
Containment Strategies
The Battle Box
Evidence Identification and Preservation
Post Event Reviews
Disaster Recovery Planning (DRP) and Business Recovery Processes
Development of BCP and DRP
Plan Development
Recovery Strategies
Basis for Recovery Strategy Selections
Disaster Recovery Sites
Recovery of Communications
Plan Maintenance Activities
BCP and DRP Training
Techniques for Testing Security
Vulnerability Assessments
Penetration Testing

Module 6 - Operations Security

Operations Security
Administrator Access
Operational Assurance
Some Threats to Computer Operations
Specific Operations Tasks
Data Leakage – Object Reuse
Object Reuse
Records Management
Change Control
Controlling How Changes Take Place
Change Control Steps
Trusted Recovery
Redundant Array of Independent Disks (RAID)
Phases of Plan
BCP Risk Analysis
Identify Vulnerabilities and Threats
Interdependencies
Identifying Functions' Resources
Calculating MTD
Recovery Point Objective
Facility Backups – Hot Site
Facility Backups – Warm Site
Facility Backups – Cold Site
Other Offsite Approaches
Priorities
OWASP Top Ten (2013)
Common Gateway Interface
How CGI Scripts Work
Cookies
Virtualization - Type 1
Virtualization – Type 2
Technologies – Databases and DBMS
Facilities
Facilities Security
Environmental Security
Physical Access Issues and Exposures
Physical Access Issues and Exposures
Physical Access Controls
Controls for Environmental Exposures
Controls for Environmental Exposures cont.
Controls for Environmental Exposures cont.
Electrical Problems
Summary

Module 7 - Network Security

Network Topologies– Physical Layer
OSI Model
An Older Model
Data Encapsulation
Protocols at Each Layer
Devices Work at Different Layers
Technology-based Security
Technologies
Security Management Report Tools
Security in Technical Components cont.
Defense in Depth
Repeater
Switch
Virtual LAN
Router
Gateway
Bastion Host
Network Security Architecture
Firewalls
Whitelisting vs. Blacklisting
Firewall Issues
Firewalls
Firewall – First line of defense
Firewall Types – Packet Filtering
Firewall Types – Proxy Firewalls
Firewall Types – Circuit-Level Proxy Firewall
Firewall Types – Application-Layer Proxy
Firewall Types – Stateful
Firewall Placement
Firewall Architecture Types – Screened Host
Firewall Architecture Types – Multi- or Dual-Homed
Firewall Architecture Types – Screened Subnet
Intrusion Detection and Prevention Systems
IDS – Second line of defense
IPS – Last line of defense?
IDS/IPS Components
IDS/IPS Features
IDS/IPS
Intrusion Detection Policies and Processes
HIPS
Unified Threat Management (UTM)
UTM Product Criteria
TCP/IP Suite
Port and Protocol Relationship
UDP versus TCP
Protocols – ARP
Protocols – ICMP
Protocols – FTP, TFTP, Telnet
Protocols – SNMP

Network Service – DNS
nslookup
IP Addressing
Network Service – NAT
Recommended NAT Addresses
Technologies - SPAM
Filtering and Content Management
Emerging Technologies
Security of Portable Media
Mobile Device Security
LAN Security Issues
Network Infrastructure Security
Client-server Security
Internet Threats and Security
Causes of Internet Attacks
Honeypots and Honeynets
LaBrea Tarpit
Voice-Over IP (VoIP)
Auditing Network Infrastructure Security
IPSec - Network Layer Protection
IPSec
IPSec
SSL/TLS
Wireless Technologies– Access Point
Standards Comparison
Wi-Fi Network Types
Wireless Technologies – Access Point
802.11i – WPA2
Wireless Security Threats
Kismet
Bluetooth
Summary