C)SLO: Certified Security Leadership Officer

Course ID #: 7000-817-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course, you will cover current security issues, best practices, and technology. With this knowledge you will then be prepared to manage the security component of an information technology project. As a Security Leadership Officer, you will be the bridge between cybersecurity and business operations. C)SLO is designed for mid and upper-level managers. If you are an engineer, this course will increase your knowledge in the leading information system security teams.

* This course/certification has been validated by the NSA for: CNSSl-4014, Information Assurance Training Standard for Information Systems Security Officers.

Course Objectives:

Upon successful completion of this course students will:

- Be able to competently take the C)SLO exam
- Be versed in implementing strong security controls and managing an organization with an industry acceptable security posture

Prerequisites:

- 12 months professional experience in IT
- 12 months professional experience in systems management

Target Audience:

- C - Level Managers
- IT Managers
- Cyber Security Personnel
- Engineers
- Information Systems
- Owners
- ISSO's
- CISSP Students
- ISO's

C)SLO: Certified Security Leadership Officer

Course ID #: 7000-817-ZZ-Z

Hours: 35

Topics:

Lesson 1 - Security Management

- The Role of the CSLO
- Business Goals and Objectives
- Overview of Governance
  - The First Priority for the CSLO
  - Outcomes of Governance
  - Performance and Governance
- Organization of IT Security
- Security Strategy
- The Goal of Information Security
- Defining Security Objectives
- Security Budget
- Security Integration
- Architecture
- Information Security Frameworks
- Integration
- COBIT 4.1
- Deming and Quality
- Ethics
- Fraud
- Hiring and Employment
- Intellectual Property
- Protecting IP
- Attacks on IP
- OECD Privacy Principles
- PII and PHI
- Awareness Training

Lesson 2 - Risk Management

- Risk Management
- Risk Assessment
- Quantitative vs Qualitative Risk
- What Is the Value of an Asset?
- What Is a Threat/Vulnerability
- Assess and Evaluate Risk
- Controls
- Comparing Cost and Benefit
- Cost of a Countermeasure
- Appropriate Controls
- Documentation

Lesson 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

C)SLO: Certified Security Leadership Officer

Course ID #: 7000-817-ZZ-Z

Hours: 35

Lesson 4 - Information Security Access Control Concepts

- Information Asset Classification
  - Criticality
  - Sensitivity
  - Regulations and Legislation
- Asset Valuation
- Information Protection
- Storing, Retrieving, Transporting and Disposing of Confidential Information
- Password Policy
- Password Cracking
- Biometrics
- Authorization
- Accounting/Auditability
- Centralized Administration
- Access Control

Lesson 5 - Incident Handling and Evidence

- Goals of Incident Management and Response
- Security Incident Handling and Response
- Evidence Handling
- What is an Incident - Intentional
- What is an Incident - Unintentional
- Malware
- Attack Vectors
- Information Warfare
- Developing Response and Recovery Plans
- Incident Response Functions
- Incident Management Technologies
- Responsibilities of the CSLO
- Crisis Communications
- Challenges in Developing an Incident Management Plan
  - a. When an Incident Occurs
  - b. During an Incident
  - c. 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
- Disaster Recovery Sites
- Recovery of Communications
- Plan Maintenance Activities
- Techniques for Testing Security
- Vulnerability Assessments
- Penetration Testing

Lesson 6 - Operations Security

- Operations Security
- Specific Operations Tasks
- Data Leakage – Object Reuse
- Records Management
- Change Control
- Trusted Recovery
- Redundant Array of Independent Disks (RAID)
- Phases of Plan
- BCP Risk Analysis
- Recovery Point Objective
- 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
- Controls for Environmental Exposures

C)SLO: Certified Security Leadership Officer

Course ID #: 7000-817-ZZ-Z

Hours: 35

Lesson 7 - Network Security

- Network Topologies– Physical Layer
- Data Encapsulation
- Protocols at Each Layer
- Devices Work at Different Layers
- Technology-based Security
- Network Security Architecture
- Firewalls
- Unified Threat Management (UTM)
- UTM Product Criteria
- TCP/IP Suite
- Port and Protocol Relationship
- Network Security
- Internet Threats and Security
- Auditing Network Infrastructure Security
- IPSec - Network Layer Protection
- Wireless Technologies– Access Point

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535