



## Diploma in Information Security Control, Audit and Management (CISSP Certification)

### Diploma in Information Security Control, Audit and Management

This course is designed and delivered by experienced information security professionals and is useful to information system managers, information security professionals or those who prepare to sit for the CISSP certification exam.

#### Course Duration:

48 hours / 8 days or 16 evenings

#### 1 Access Control Systems and Methodology

- Access Control Overview
  - Types of Access Control
  - Access Control in a Layered Environment
  - The Process of Accountability
- Identification and Authentication Techniques
  - Passwords
  - Biometrics
  - Tokens
  - Tickets
- Access Control Techniques
- Access Control Methodologies and

#### Implementation

- Centralized and Decentralized Access Control
- RADIUS and TACACS
- Access Control Administration
  - Account Administration
  - Account, Log, and Journal Monitoring
  - Access Rights and Permissions
- Access Control Working Process

#### 2 Attacks and Monitoring

- Monitoring
- Intrusion Detection
  - Host-Based and Network-Based IDSs
  - Knowledge-Based and Behavior-Based Detection
- IDS-Related Tools
- Penetration Testing
- Methods of Attacks
  - Brute Force and Dictionary Attacks
  - Denial of Service
  - Spoofing Attacks
  - Man-in-the-Middle Attacks
  - Sniffer Attacks
  - Spamming Attacks
  - Crackers
- Access Control Compensations

#### 3 ISO Model, Network Security, and Protocols

- Security Testing Working Process
- OSI Model
  - History of the OSI Model
  - OSI Functionality
  - Encapsulation / Deencapsulation
  - OSI Layers
  - TCP/IP Model
- Communications and Network Security
  - Network Cabling
  - LAN Technologies
  - Network Topologies
  - TCP/IP Overview
- Internet/Intranet/Extranet Components
  - Firewalls
  - Other Network Devices
- Remote Access Security Management
- Network and Protocol Security Mechanisms
  - VPN Protocols
  - Secure Communications Protocols
  - E-Mail Security Solutions
  - Dial-Up Protocols
  - Authentication Protocols
  - Centralized Remote Authentication Services
- Network and Protocol Services
  - Frame Relay

- Other WAN Technologies
- Avoiding Single Points of Failure
  - Redundant Servers
  - Failover Solutions
  - RAID
- Security Audit Working Process

#### 4 Communications Security and Countermeasures

- Virtual Private Network (VPN)
  - Tunneling
  - How VPNs Work
  - Implementing VPNs
- Network Address Translation
  - Private IP Addresses
  - Stateful NAT
- Switching Technologies
  - Circuit Switching
  - Packet Switching
  - Virtual Circuits
- WAN Technologies
  - WAN Connection Technologies
  - Encapsulation Protocols
- Miscellaneous Security Control Characteristics
  - Transparency
  - Verifying Integrity
  - Transmission Mechanisms
- Managing E-Mail Security
  - E-Mail Security Goals
  - Understanding E-Mail



## Diploma in Information Security Control, Audit and Management (CISSP Certification)

- Security Issues
  - E-Mail Security Solutions
  - Securing Voice Communications
    - Social Engineering
    - Fraud and Abuse
    - Phreaking
  - Security Boundaries
  - Network Attacks and Countermeasures
    - Eavesdropping
    - Second-Tier Attacks
    - Address Resolution Protocol (ARP)
  - IT Audit Working Process
- 5 Security Management Concepts and Principles**
- Confidentiality
  - Integrity
  - Availability
  - Other Security Concepts
  - Protection Mechanisms
    - Layering
    - Abstraction
    - Data Hiding
    - Encryption
  - Change Control/Management
  - Data Classification
  - IT Audit Working Process
- 6 Asset Value, Policies, and Roles**
- Employment Policies and Practices
    - Security Management for Employees
- Security Roles
  - Policies, Standards, Baselines, Guidelines, and Procedures
    - Security Policies
    - Security Standards, Baselines, and Guidelines
    - Security Procedures
  - Risk Management
    - Risk Terminology
    - Risk Assessment Methodologies
    - Quantitative Risk Analysis
    - Qualitative Risk Analysis
    - Handling Risk
  - Security Awareness Training
  - Security Management Planning
  - IT Security Audit Working Process
  - Exam Essentials
  - Review Questions
  - Answers to Review Questions
- 7 Data and Application Security Issues**
- Application Issues
    - Local/Nondistributed Environment
    - Distributed Environment
  - Databases and Data Warehousing
    - Database Management
- System (DBMS) Architecture
    - Database Transactions
    - Multilevel Security
    - Aggregation
    - Inference
    - Polyinstantiation
    - Data Mining
  - Data/Information Storage
    - Types of Storage
    - Storage Threats
  - Knowledge-Based Systems
    - Expert Systems
    - Neural Networks
    - Security Applications
  - Systems Development Controls
  - Software Development Life Cycle
    - Systems Development
    - Life Cycle Models
    - Change Control and Configuration Management
    - Security Control Architecture
    - Service Level Agreements
  - Data and Application Security Audit Working Process
- 8 Malicious Code and Application Attacks**
- Malicious Code
    - Sources
    - Viruses
- Logic Bombs
  - Trojan Horses
  - Worms
  - Active Content
  - Countermeasures
  - Password Attacks
    - Password Guessing
    - Dictionary Attacks
    - Social Engineering
    - Countermeasures
  - Denial of Service Attacks
    - SYN Flood
    - Distributed DoS Toolkits
    - Smurf
    - Teardrop
    - Land
    - DNS Poisoning
    - Ping of Death
  - Application Attacks
    - Buffer Overflows
    - Time-of-Check-to-Time-of-Use
    - Trap Doors
    - Rootkits
  - Reconnaissance Attacks
    - IP Probes
    - Port Scans
    - Vulnerability Scans
    - Dumpster Diving
  - Masquerading Attacks
    - IP Spoofing
    - Session Hijacking
  - Decoy Techniques
    - Honey Pots
    - Pseudo-Flaws
- 9 Cryptography and Private**



## Diploma in Information Security Control, Audit and Management (CISSP Certification)

### Key Algorithms

- History
  - Caesar Cipher
  - Ultra vs. Enigma
- Cryptographic Basics
  - Goals of Cryptography
  - Concepts
  - Cryptographic Mathematics
  - Ciphers
- Modern Cryptography
  - Cryptographic Keys
  - Symmetric Key Algorithms
  - Asymmetric Key Algorithms
  - Hashing Algorithms
- Symmetric Cryptography
  - Data Encryption Standard (DES)
  - Triple DES (3DES)
  - International Data Encryption Algorithm (IDEA)
  - Blowfish
  - Skipjack
  - Advanced Encryption Standard (AES)
  - Key Distribution
  - Key Escrow

### 10 PKI and Cryptographic Applications

- Asymmetric Cryptography
  - Public and Private Keys
  - RSA
  - El Gamal

- Elliptic Curve
- Hash Functions
  - SHA
  - MD2
  - MD4
  - MD5
- Digital Signatures
  - HMAC
  - Digital Signature Standard
- Public Key Infrastructure
  - Certificates
  - Certificate Authorities
  - Certificate Generation and Destruction
  - Key Management
- Applied Cryptography
  - Electronic Mail
  - Web
  - E-Commerce
  - Networking
- Cryptographic Attacks

### 11 Security Protection Mechanisms

- Technical Mechanisms
- Security Policy and Computer Architecture
- Policy Mechanisms
- Distributed Architecture
- Security Models
  - State Machine Model
  - Bell-LaPadula Model
  - Biba
  - Clark-Wilson
  - Information Flow Model
  - Noninterference Model

- Take-Grant Model
- Access Control Matrix
- Brewer and Nash Model (a.k.a. Chinese Wall)
- Classifying and Comparing Models

### 12 Principles of Security Models

- Common Security Models, Architectures, and Evaluation Criteria
  - Trusted Computing Base (TCB)
  - Security Models
  - Objects and Subjects
  - Closed and Open Systems
  - Techniques for Ensuring Confidentiality, Integrity, and Availability
    - Controls
    - IP Security (IPSec)
- Understanding System Security Evaluation
  - Rainbow Series
  - ITSEC Classes and Required Assurance and Functionality
  - Common Criteria
  - Certification and Accreditation
- Common Flaws and Security Issues
  - Covert Channels

- Attacks Based on Design or Coding Flaws and Security Issues
- Programming
- Timing, State Changes, and Communication Disconnects
- Electromagnetic Radiation

### 13 Administrative Management

- Antivirus Management
- Operations Security Concepts
  - Operational Assurance and Life Cycle Assurance
  - Backup Maintenance
  - Changes in Workstation/Location
  - Need-to-Know and the Principle of Least Privilege
  - Privileged Operations Functions
  - Trusted Recovery
  - Configuration and Change Management Control
  - Standards of Due Care and Due Diligence
  - Privacy and Protection
  - Legal Requirements
  - Illegal Activities
  - Record Retention
  - Sensitive Information and Media



## Diploma in Information Security Control, Audit and Management (CISSP Certification)

- Security Control Types
- Operations Controls
- Personnel Controls

### 14 Auditing and Monitoring

- Auditing
  - Auditing Basics
  - Audit Trails
  - Reporting Concepts
  - Sampling
  - Record Retention
  - External Auditors
- Monitoring
  - Monitoring Tools and Techniques
- Penetration Testing Techniques
  - War Dialing
  - Sniffing and Eavesdropping
  - Radiation Monitoring
  - Dumpster Diving
  - Social Engineering
  - Problem Management
- Inappropriate Activities
- Indistinct Threats and Countermeasures
  - Errors and Omissions
  - Fraud and Theft
  - Collusion
  - Sabotage
  - Loss of Physical and Infrastructure Support
  - Malicious Hackers or Crackers
  - Espionage
  - Malicious Code

- Traffic and Trend Analysis
- Initial Program Load Vulnerabilities

### 15 Business Continuity Planning

- Business Continuity Planning
- Project Scope and Planning
  - Business Organization Analysis
  - BCP Team Selection
  - Resource Requirements
  - Legal and Regulatory Requirements
- Business Impact Assessment
  - Identify Priorities
  - Risk Identification
  - Likelihood Assessment
  - Impact Assessment
  - Resource Prioritization
- Continuity Strategy
  - Strategy Development
  - Provisions and Processes
  - Plan Approval
  - Plan Implementation
  - Training and Education
- BCP Documentation
  - Continuity Planning Goals
  - Statement of Importance
  - Statement of Priorities
  - Statement of Organizational

- Responsibility
- Statement of Urgency and Timing
- Risk Assessment 464 Risk
- Acceptance/Mitigation
- Vital Records Program
- Emergency Response Guidelines
- Maintenance
- Testing
- IT Audit Working Process

### 16 Disaster Recovery Planning

- Disaster Recovery Planning
  - Natural Disasters
  - Man-Made Disasters
- Recovery Strategy
  - Business Unit Priorities
  - Crisis Management
  - Emergency Communications
  - Work Group Recovery
  - Alternate Processing Sites
  - Mutual Assistance Agreements
  - Database Recovery
- Recovery Plan Development
  - Emergency Response
  - Personnel Notification
  - Backups and Offsite Storage
  - Software Escrow Arrangements
  - External

- Communications
- Utilities
- Logistics and Supplies
- Recovery vs. Restoration
- Training and Documentation
- Testing and Maintenance
  - Checklist Test
  - Structured Walk-Through
  - Simulation Test
  - Parallel Test
  - Full-Interruption Test
  - Maintenance

### 17 Law and Investigations

- Categories of Laws
  - Criminal Law
  - Civil Law
  - Administrative Law
- Laws
  - Computer Crime
  - Intellectual Property
  - Licensing
  - Import/Export
  - Privacy
- Investigations
  - Evidence
  - Investigation Process

### 18 Incidents and Ethics

- Major Categories of Computer Crime
  - Military and Intelligence Attacks
  - Business Attacks
  - Financial Attacks
  - Terrorist Attacks



## Diploma in Information Security Control, Audit and Management (CISSP Certification)

---

- Grudge Attacks
- "Fun" Attacks
- Evidence
- Incident Handling
  - Common Types of Incidents
  - Response Teams
  - Abnormal and Suspicious Activity
  - Confiscating Equipment, Software, and Data
  - Incident Data Integrity and Retention
  - Reporting Incidents
- Ethics
  - Code of Ethics
  - Ethics and the Internet

### 19 Physical Security Requirements

- Facility Requirements
    - Secure Facility Plan
    - Physical Security Controls
    - Site Selection
    - Visibility
    - Accessibility
    - Natural Disasters
    - Facility Design
    - Work Areas
    - Server Rooms
    - Visitors
  - Forms of Physical Access Controls
    - Fences, Gates, Turnstiles, and Mantraps
    - Lighting
- Security Guards and Dogs
  - Keys and Combination Locks
  - Badges
  - Motion Detectors
  - Intrusion Alarms
  - Secondary Verification Mechanisms
  - Technical Controls
    - Smart Cards
    - Proximity Readers
    - Access Abuses
    - Intrusion Detection Systems
    - Emanation Security
  - Environment and Life Safety
    - Personnel Safety
    - Power and Electricity
    - Noise
    - Temperature, Humidity, and Static
    - Water
    - Fire Detection and Suppression