CISSP: Certified Information Systems Security Professional - 2018 Edition

Course Overview

This course will teach students about security and risk management, asset management, security architecture and engineering, communication and network security, identity and access management, security assessment and testing, security operations, and software development security.

Course Introduction 15m
Course Introduction

Domain 01 - Security and Risk Management 3h 7m
Topic: Confidentiality, Integrity, and Availability
Confidentiality
Integrity
Availability
References
Topic: Security Governance
Security Governance Principles
Security Functions to Business Goals
Organizational Processes
Roles and Responsibilities
Security Control Frameworks
Due Care / Due Diligence
References
Topic: Compliance Requirements
Compliance Requirements
Contracts, Legal, Industry Standards
Privacy Requirements
References
Topic: Legal and Regulatory - Global
Legal and Regulatory - Global
Cyber Crimes and Data Breaches
Intellectual Property
Import / Export Controls
Trans-border Data Flows
Privacy
References
Topic: Professional Ethics
Professional Ethics
Topic: Security Policy, Standards, Procedures
Security Policy, Standards, Procedures
References
Topic: Business Continuity
Business Continuity

Document Scope and Plan
Business Impact Analysis
References
Topic: Personal Security Policies
Personal Security Policies
Candidate Screening / Hiring
Employment Agreements / Polices
On-boarding / Termination Process
Vendor, Consultant, Contractor
Compliance Policy Requirements
Privacy Policy Requirements
References
Topic: Apply Risk Management
Apply Risk Management
References
Topic: Threat Modeling
Threat Modeling – Concepts / Methodology
Threat Modeling – Categorizing Threats
Threat Modeling – Generic Steps
Threat Modeling – Analyzing Risk
References
Topic: Risk Management – Supply Chain
Risk Management – Hardware, Software
Risk Management – 3rd Party Evaluations
Risk Management – Minimum Security
References
Topic: Security Awareness and Training
Security Awareness and Training
Methods and Techniques
Periodic Content Reviews
Effectiveness Evaluations
References

Domain 02 - Asset Management 1h 24m
Topic: Identify and Classify
Data Classification
Asset Classification
References
Topic: Asset Ownership
Asset Ownership
References
Topic: Protect Privacy
Data Owners
Data Processors
Data Remanence
Data Collection
References
Topic: Asset Retention
Asset Retention
Record Retention

References
Topic: Data Security Controls
Data Security Controls
Scoping and Tailoring
Standards Selection
Data Protection Methods
References
Topic: Information / Asset Handling
Information / Asset Handling
Failure Examples
Storage Options
References

Domain 03 - Security Architecture and Engineering 2h 57m
Topic: Engineering Processes and Secure Design
Engineering Processes and Secure Design
Closed / Open Systems
Closed / Open Source Code
Techniques / Confinement
Bounds
Process Isolation
Controls / MAC and DAC
References
Topic: Concepts of Security Models
Concepts of Security Models
Security Perimeter
Reference Monitors / Security Kernels
Various Models
References
Topic: Controls Based on Security Requirements
Controls Based on Security Requirements
Rainbow Series
TCSEC
ITSEC / Common Criteria
Common Criteria
References
Topic: Security Capabilities of Information Systems
Security Capabilities of Information Systems
Virtualization
Trusted Platform Module
References
Topic: Assess / Mitigate Vulnerabilities
Assess / Mitigate Vulnerabilities
Local Caches
Server-Based Systems
Database Systems
Industrial Control Systems
Cloud-Based Systems
Distributed Systems
Internet of Things

References
Topic: Assess / Mitigate Vulnerabilities (Web)
Assess / Mitigate Vulnerabilities (Web)
References
Topic: Assess / Mitigate Vulnerabilities (Mobile)
Assess / Mitigate Vulnerabilities (Mobile)
Device Security
Application Security
References
Topic: Assess / Mitigate Vulnerabilities (Embedded)
Assess / Mitigate Vulnerabilities (Embedded)
Embedded / Static Systems
Securing Embedded / Static Systems
References
Topic: Apply Cryptography
Apply Cryptography
Cryptographic Life Cycle
Cryptographic Methods
Symmetric Key
Asymmetric Key
Elliptic Curve
Public Key Infrastructure
Certificates
Key Management
Digital Signatures
Integrity - Hashing
Cryptanalytic Attacks
Digital Rights Management (DRM)
References
Topic: Site / Facility Security Principles
Site / Facility Security Principles
References
Topic: Site / Facility Security Controls
Site / Facility Security Controls
Server Rooms / Data Centers
Media Storage Facilities
Evidence Storage
Restricted and Work Area Security
Utilities and HVAC
Environmental Issues
Fire Prevention, Detection, and Suppression
Fire Extinguishers / Detection
Water Suppression / Gas Discharge
References

Domain 04 - Communication and Network Security 1h 2m
Topic: Secure Design and Network Architecture
Secure Design and Network Architecture
OSI Model
Encapsulation / Decapsulation

Physical / Data Link Layers
Network Layer
Transport Layer
Session Layer
Presentation Layer
Application Layer
IP Networking
TCP/IP
SYN / ACK / TCP
IP Classes
Multilayer Protocols
Converged Protocols
Wireless Networks
Secure SSID
Secure Encryption Protocols
References
Topic: Secure Network Components
Operation of Hardware
Firewalls
Firewall Inspection
Transmission Media
Baseband / Broadband
Twisted Pair
Network Access Controls
Network Access Controls - Concepts
Endpoint Security
Distribution Networks
References
Topic: Secure Communication Design
Voice
PBX Fraud
Multimedia Collaboration
Remote Meeting
Securing Email
Remote Access
Remote Authentication
Virtualized Networks
VPN Protocols
References

Domain 05 - Identity and Access Management 1h 14m
Topic: Physical and Logical Access
Information
Access Control Process
Logical and Technical Access Controls
Systems
Devices
Facilities
References
Topic: Manage Identification / Authentication

Identity Implementation
Single / Multi-factor Authentication
Service Authentication
Accountability
Session Management
Registration / Proofing Identity
Federated Identity Management
Common Language
Credential Management Systems
CyberArk
References
Topic: Integrate Identity as a Third-Party Service
On-Premise
Cloud
Federated
References
Topic: Implement and Manage Authorization
Role-Based Access
Upsides / Downsides
Rule-Based Access
Mandatory Access
Discretionary Access
Attribute-based Access
References
Topic: Manage Identity / Access Lifecycle
Account Review
System Access Review
Provisioning
References

Domain 06 - Security Assessment and Testing 1h 14m
Topic: Assessment, Test, and Audit Strategies
Assessment, Test, and Audit Strategies
Security Assessment / Testing
Security Assessments
External / Third Party
Auditing Standards
References
Topic: Security Control Testing
Vulnerability Assessment
Vulnerability Scans
Network Vulnerability Scans
Web Vulnerability Scans
Penetration Testing
Testing Options
Log Reviews
Synthetic Transaction
Code Review / Testing
Testing Options (cont.)
Misuse Case Testing

Test Coverage Analysis
Interface Testing
References
Topic: Security Process Data
Account Management
Management Review
Performance and Risk Indicators
Backup Verification
Training and Awareness
References
Topic: Analyze Test Output / Generate Reports
Analyze Test Output / Generate Reports
External Scan Report
References
Topic: Conduct / Facilitate Security Audit
Internal Aspects
External / 3rd Party Aspect
References

Domain 07 - Security Operations 3h 21m
Topic: Investigations
Evidence Collection
Network / Software / Hardware Analysis
Reporting and Documentation
Investigative Techniques
Gathering Evidence
Digital Forensics
Chain of Custody
References
Topic: Investigation Team
Administrative Aspects
Criminal Investigations
Civil Investigations
Regulatory Investigations
References
Topic: Logging and Monitoring Activities
SIEM
Deployment
Continuous Monitoring
Egress Monitoring
Tools to Assist
References
Topic: Provisioning Resources
Asset Inventory
Asset Management
Cloud-Based Management
Configuration Management
References
Topic: Security Operations Concepts
Separation of Duties

Need to Know / Least Privilege
Separation of Privilege
Privileged Account Management
Job Rotation
Information Lifecycle
Key Phases of Data
Service Level Agreements
References
Topic: Protection Techniques
Media Management
Hardware / Software Asset Management
Software
References
Topic: Incident Management
Detection
Responsive
Reporting
Legal / Compliance
Recovery
Remediation
Lessons Learned
References
Topic: Detective / Preventative Measures
Firewalls
Intrusion Detection / Prevention
Knowledge / Behavior-Based
Network / Host-Based
Whitelisting / Blacklisting
Third-Party Security Services
Sandboxing
Honeypots/Honeynets
Anti-Malware
References
Topic: Patch and Vulnerability Management
Patch / Vulnerability Management
Patch Management
References
Topic: Change Management Processes
Change Management
Security Impact Analysis
References
Topic: Implement Recovery Strategies
Backup Storage
Recovery Site Strategies
Business / Functional Unit Priorities
Crisis Management
Multiple Processing Sites
Options
Cloud Computing
High Availability / QoS

Hard Drives / Power Sources
QoS
References
Topic: Implement Disaster Recovery
Response
Personnel
Communications
Assessment
Restoration
Training and Awareness
References
Topic: Test Disaster Recovery
Overview
Read-Through Checklists
Walk-Through (Table-Top)
Simulation Test
Parallel Test
Full Interruption
References
Topic: Implement / Manage Physical Security
Perimeter Security
Fences, Gates and Lighting
Security Dogs
Internal Security Controls
Badges / Regulatory Requirements
References
Topic: Personnel Safety / Security
Travel
Security Training and Awareness
Emergency Management
Duress
References

Domain 08 - Software Development Security 1h 5m

Topic: Software Development Life Cycle
Development Methodologies
Functional Requirements / Control Specifications
Design / Code Review
User Acceptance Testing / Change Management
Maturity Models
Agile / SW-CMM
Change Management
Integrated Product Team
References
Topic: Security Controls in Development
Security of Software Environments
Development Security
Secure Coding Configuration Management
Code Repositories
Best Practices

References
Topic: Assess Software Security Effectiveness
Auditing and Logging
ODBC / NoSQL
Risk Analysis / Mitigation
Development Methodology
Tracking Progress / Repeat
References
Topic: Security Impact of Acquired Software
Security Impact of Acquired Software
OWASP Key Considerations
References
Topic: Secure Coding Guidelines and Standards
Security Weaknesses / Vulnerabilities
Reconnaissance Attacks
Masquerading Attacks
API Security
Secure Coding Practices
Testing Options
References
Course Closure

Total Duration: 15h 38m