

CISSP: Certified Information Systems Security Professional

Course Overview

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

Course Introduction

13m

Course Introduction
Instructor Introduction
Experience Requirements
Examination Information - CAT
Examination Information - Linear
Examination Retakes
Domains Average Weight
Exam Tips - CAT
Domain 1 - Security and Risk Management
Domain 2 - Asset Security
Domain 3 - Security Architecture and Engineering
Domain 4 - Communication and Network Security
Domain 5 - Identity and Access Management
Domain 6 - Security Assessment and Testing
Domain 7 - Security Operations
Domain 8 - Software Development Security
Examination Policies and Procedures
References

Domain 1 - Security and Risk Management

2h 2m

Security and Risk Management
Topic: Professional Ethics
Ethics
(ISC)2 Code of Professional Ethics
Organizational Code of Ethics
References
Topic: Security Concepts
Security Terminology
Information Security
Cybersecurity
Asset
Vulnerability
Threat
Risk
Subject
Object

CIA Triad
Confidentiality
Confidentiality
Confidentiality
Integrity
Integrity
Availability
Availability
DAD Triad
DAD Triad
AAA Services
Protection Mechanisms
Layering/Defense in Depth
Abstraction
Data Hiding
Encryption
References
Topic: Security Governance Principles
Governance
Information Security Governance
Security Governance vs Security Management
Third-Party Governance
Documentation Review
References
Topic: Security Function
Alignment of Security Function
Alignment to Strategy, Goals, Mission, and Objectives
Security Policy
Top-Down Approach
Management Approval
Security Management
Security Management Plans
Organizational Processes
Organizational Roles and Responsibilities
Organizational Roles and Responsibilities (Cont.)
Security Control Frameworks
Due Care and Due Diligence
References
Topic: Policy, Standards, Procedures, and Guidelines
Topic: Personnel Security
Personnel Management
Employment
Screening and Hiring
Onboarding, Offboarding, and Termination
Transfers
Agreements, Policies, and Procedures
Vendor, Consultant, and Contractor Controls
Compliance
Privacy
Security Awareness, Education, and Training

References

Topic: Risk Management Concepts

Risk Management

Risk Terminologies

Risk Terminologies

Threats and Vulnerabilities Identification

Risk Analysis/Assessment

Quantitative Risk Analysis

Quantitative Risk Analysis

Qualitative Risk Analysis

Qualitative Risk Analysis

Risk Responses

Safeguard/Countermeasure Selection

Safeguard/Countermeasure Implementation

Types of Controls

Security Control Assessment

Monitoring and Measuring

Risk Reporting

Continuous Improvement

Risk Frameworks

References

Topic: Threat Modeling

Threat Modeling

Identifying Threats

Threat Schemes and Models

Security Development Lifecycle (SDL)

STRIDE

PASTA

Others Threat Models

Determining and Diagramming Potential Attacks

Performing Reduction Analysis

Prioritization and Response

DREAD

References

Topic: Supply Chain Risk Management

Topic: Business Continuity Planning

Project Scope and Planning

Business Impact Assessment

Continuity Planning

Approval and Implementation

References

Topic: Compliance, Legal, and Regulatory Issues

Categories of Laws

Laws

Computer Crime

Intellectual Property

Licensing

Import/Export

Privacy

Privacy

State Privacy Laws
Compliance
Contracting and Procurement
References
Domain 1 Review
Domain 1 Review

Domain 2 - Asset Security

38m

Asset Security
Topic: Asset Identification and Classification
Defining Sensitive Data
Data Classification
Data Classification - Government/Military
Data Classification
Data Classification - Government/Military
Data Classification - Non-government/Civilian
Asset Classification
Data States
References
Topic: Asset Ownership and Handling Requirements
Data Roles
Data Roles
Asset Handling Requirements
Data Maintenance
Marking and Labeling
Data Loss Prevention
References
Topic: Asset and Data Management
Handling Information and Assets
Eliminating Data Remanence
Eliminating Data Remanence (Cont.)
Data and Asset Retention
References
Topic: Security Controls and Compliance Requirements
Using Security Baselines
NIST SP 800-53B
Tailoring and Scoping
Standards Selection
Data Security Controls
References
Domain 2 Review
Domain 2 Review

Domain 3 - Security Architecture and Engineering

2h 42m

Security Architecture and Engineering
Topic: Fundamental Security Engineering Processes and Secure Design Principles
Objects and Subjects
Open and Closed Systems
Open and Closed Source
Techniques for Ensuring Confidentiality, Integrity, and Availability

Controls

Trust and Assurance

References

Topic: Security Models

Trusted Computing Base

State Machine Model

Information Flow Model and Noninterference Model

Bell-LaPadula Model

Biba Model

Bell-LaPadula vs Biba Model

Clark-Wilson Model

Other Security Models

References

Topic: Controls Selection

Rainbow Series

Evaluation Models

Evaluation Models (Cont.)

Certification and Accreditation

References

Topic: Security Capabilities of Information Systems

Memory Protection

Virtualization

Trusted Platform Module (TPM)

Interfaces

Fault Tolerance

References

Topic: Vulnerability Management in Security Architectures, Designs, and Solution Elements

Hardware

Hardware

Firmware

Client-Based

Server-Based Systems

Distributed Systems

High-Performance Computing (HPC) Systems

Serverless, Containerization, and Cloud-Based Systems

Edge and Fog Computing

Industrial Control Systems

Endpoint, Embedded Devices, and Cyber-Physical Systems

Critical Security Protection Mechanisms

Common Architecture Flaws and Security Issues

References

References

Topic: Cryptographic Concepts, Solutions, and Attacks

Foundations

Goals of Cryptography

Cryptography Concepts

Cryptography Concepts

Cryptographic Mathematics

Codes and Ciphers

References

Modern Cryptography
Hashing
Symmetric Key Cryptography
Symmetric Key Cryptography (Cont.)
Symmetric Key Cryptography (Cont.)
Asymmetric Key Cryptography
Asymmetric Key Cryptography (Cont.)
Asymmetric Key Cryptography (Cont.)
Asymmetric Key Cryptography (Cont.)
Asymmetric Key Cryptography (Cont.)
Cryptographic Life Cycle
References
Applied Cryptography
References
Cryptographic Attacks
Cryptographic Attacks (Cont.)
References
Topic: Site and Facility Selection, Design, and Security Controls
Security Principles for Site and Facility Design
Site and Facility Security Controls
Site and Facility Security Controls (Cont.)
Site and Facility Security Controls (Cont.)
Physical Security
References
Domain 3 Review
Domain 3 Review

Domain 4 - Communication and Network Security

1h 39m

Communication and Network Security
Topic: Secure Network Architecture and Design
Security Boundaries
Protocol Security
Secure Communication Protocols
IPsec
Kerberos
Secure Shell (SSH)
Signal Protocol
Secure Remote Procedure Call (S-RPC)
Transport Layer Security (TLS)
Authentication Protocols
Password Authentication Protocol (PAP)
Challenge-Handshake Authentication Protocol (CHAP)
Extensible Authentication Protocol (EAP)
Internet Protocol
IPv4 and IPv6
IP Classes
VLSM and CIDR
ICMP and IGMP
Topology Communication Technologies
Network Topologies

Transmission Media
Transmission Media (Cont.)
LAN Technologies
Ethernet
Analog and Digital
Synchronous and Asynchronous
Baseband and Broadband
Broadcast, Multicast, and Unicast
LAN Media Access
Carrier-Sense Multiple Access (CSMA)
Token Passing
Polling
Site Survey
References
References
Topic: Models, Devices, and Protocols
OSI Model
Encapsulation / Decapsulation
OSI Layers
OSI Layers (Cont.)
OSI Layers (Cont.)
OSI Layers (Cont.)
OSI Layers (Cont.)
TCP/IP Model
Secure Protocols
Converged Protocols
Wireless Networks and Security
Wireless Networks and Security (Cont.)
Wireless Networks and Security (Cont.)
Cellular Networks
Cellular Networks (Cont.)
Firewalls
Firewall Deployment Architectures
Network Access Control
References
Topic: Secure Communications Design and Technologies
Secure Communication Protocols
Voice and Multimedia
Voice and Multimedia (Cont.)
Email Security
Remote Access Management
Remote Access Management (Cont.)
Virtual Private Network
Switching Technologies
WAN
Common Network Attacks
References
Domain 4 Review
Domain 4 Review

Domain 5 - Identity and Access Management

1h 38m

Identity and Access Management

Topic: Physical and Logical Access Control

Physical and Logical Access

Defense-in-Depth

CIA Triad and Access Controls

References

Topic: Authentication Methods

Subjects and Objects

Recap: AAA Services

Authorization

Accounting

Authentication Factors

Authentication Factors (Cont.)

Type 1 Authentication Factor - Something You Know

Type 2 Authentication Factor - Something You Have

Type 3 Authentication Factor - Something You Are

Types of Authentication

Multifactor Authentication (MFA)

Passwordless Authentication

Device Authentication

Service Authentication

Mutual Authentication

References

Topic: Identity, Federation, and Third-Party Identity Services

Centralized and Decentralized Access Control

Single Sign-On

SSO and Identity Federation

Credential Management

Scripted Access

Session Management

References

Topic: Access Control Models

Permissions, Rights, and Privileges

Authorization Mechanisms

Authorization Mechanisms (Cont.)

Security Policy

Access Control Models

Discretionary Access Control (DAC)

Nondiscretionary Access Control

Role-Based Access Control (RBAC)

Rule-Based Access Control (RuBAC)

Attribute-Based Access Control (ABAC)

Mandatory Access Control (MAC)

Risk-Based Access Control

References

Topic: Identity and Access Lifecycle

Topic: Authentication Systems

SSO and the Internet

Extensible Markup Language (XML)

Security Assertion Markup Language (SAML)
OAuth
OpenID
OpenID Connect (OIDC)
SSO and the Internal Networks
AAA Protocols
Kerberos
Kerberos (Cont.)
RADIUS
DIAMETER
TACACS+
References
References
Topic: Access Control Attacks
Crackers vs Hackers
Common Attacks
Common Attacks
Topic: Protection Methods
Domain 5 Review
Domain 5 Review

Domain 6 - Security Assessment and Testing

35m

Security Assessment and Testing
Topic: Security Assessments, Tests, and Audit Strategies
Security Testing
Security Testing (Cont.)
Security Assessments
Security Audits
References
Topic: Security Control Testing
Vulnerability Assessments
Describing Vulnerabilities
Security Content Automation Protocol (SCAP)
Vulnerability Scanning
Network Discovery Scanning
Network Vulnerability Scanning
Web Vulnerability Scanning
Database Vulnerability Scanning
Penetration Testing
Penetration Testing (Cont.)
Software Testing
Code Review and Testing
Code Review and Testing (Cont.)
Interface Testing
Misuse Case Testing
Test Coverage Analysis
Website Monitoring
References
Topic: Security Processes Data Collection and Reporting
Security Processes Data Collection and Reporting

Security Processes Data Collection and Reporting (Cont.)

References

Topic: Security Audits

Categories of Audits

Auditing Standards

System and Organization Controls (SOC)

Compliance Checks

References

Domain 6 Review

Domain 6 Review

Domain 7 - Security Operations

1h 18m

Security Operations

Topic: Foundational Security Operations Concepts

Need to Know and Principle of Least Privilege

Separation of Duties/Responsibilities, Two-Person Control, and Split Knowledge

Job Rotation and Mandatory Vacations

Privileged Account Management and Service Level Agreements

References

Topic: Personnel Safety and Security

References

Topic: Provisioning Resources

Ownership

Asset Management and Protection

References

Topic: Configuration, Change, Patch, and Vulnerability Management

Configuration Management

Change Management

Patch and Vulnerability Management

References

Incident Management and Response

Defining Incident

Incident Response Steps

Incident Response Steps (Cont.)

References

Topic: Detective and Preventive Measures

Intrusion Detection and Prevention Systems

Preventive Measures

Attacks

Attacks

Attacks

References

Topic: Logging and Monitoring

Logging and Monitoring Techniques

Role of Monitoring

Automating Incident Response

Automating Incident Response (Cont.)

References

Topic: Developing, Testing, Implementing, and Maintaining BCP and DRP

Nature of Disaster

Resilience, High Availability, and Fault Tolerance
Resilience, High Availability, and Fault Tolerance (Cont.)
Recovery Strategies
Recovery Strategies (Cont.)
Planning
Testing and Maintenance
Documentation and Training
References
Topic: Investigations and Ethics
Investigations
Investigation Types
Evidence
Evidence (Cont.)
Major Categories of Computer Crime
Ethics
Organizational Code of Ethics
(ISC)2 Code of Ethics
Ethics and the Internet
References
Domain 7 Review
Domain 7 Review

Domain 8 - Software Development Security

47m

Software Development Security
Topic: Systems Development Controls
Systems Development Lifecycle
Lifecycle Models
Waterfall Model
Spiral Model
Agile
Capability Maturity Model (CMM)
IDEAL Model
Change Management and Configuration Management
Service-Level Agreements
Third-Party Software Acquisition
References
Topic: Programming Languages and Concepts
Programming Languages
Libraries
Application Programming Interface (API)
DevOps
References
Topic: Security Controls in Software Development
Code Security
Database Security
Database Security (Cont.)
Web Application Firewall (WAF)
References
Topic: Secure Coding Standards and Guidelines
Source Code Comments

Error/Exception Handling
Hard-Coded Credentials
Memory Management
References
Topic: Software Testing, Assurance, and Vulnerabilities
Software Testing
Software Assurance (SwA)
Vulnerabilities
Types of Malware
Sources of Malware
Types of Attacks
Password Attacks
Application Attacks
Web Application Attacks
Reconnaissance Attacks
Masquerading Attacks
Zero-Day Attacks
References
Domain 8 Review
Domain 8 Review

Course Review

1h 2m

Certified Information Systems Security Professional
Domains Average Weight
Domain 1 - Security and Risk Management
Domain 1 - Security and Risk Management
Domain 1 - Security and Risk Management
Domain 1 - Security and Risk Management
Domain 1 - Security and Risk Management
Domain 1 - Security and Risk Management
Domain 1 - Security and Risk Management
Domain 2 - Asset Security
Domain 2 - Asset Security
Domain 2 - Asset Security
Domain 3 - Security Architecture and Engineering
Domain 3 - Security Architecture and Engineering
Domain 3 - Security Architecture and Engineering
Domain 3 - Security Architecture and Engineering
Domain 3 - Security Architecture and Engineering
Domain 4 - Communication and Network Security
Domain 4 - Communication and Network Security
Domain 4 - Communication and Network Security
Domain 4 - Communication and Network Security
Domain 5 - Identity and Access Management
Domain 5 - Identity and Access Management
Domain 5 - Identity and Access Management
Domain 5 - Identity and Access Management
Domain 5 - Identity and Access Management
Domain 6 - Security Assessment and Testing
Domain 6 - Security Assessment and Testing

Domain 6 - Security Assessment and Testing

Domain 7 - Security Operations

Domain 7 - Security Operations

Domain 7 - Security Operations

Domain 7 - Security Operations

Domain 7 - Security Operations

Domain 8 - Software Development Security

Domain 8 - Software Development Security

Domain 8 - Software Development Security

Domain 8 - Software Development Security

EXAM TIPS

EXAM TIPS

Total Duration: 12h 33m