(ISC)² CISSP – Certified Information Systems Security Professional - 2021

This CISSP training course maps to the CISSP methodology exam objectives and prepares learners to design, implement, and maintain your organization's cybersecurity programs. After finishing this CISSP certification training, you'll have a broad understanding of the eight domains of the CISSP CBK, be ready to take on the CISSP exam, and be in a good position to move into more senior-level security roles.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Information Security: Security and Risk Management

CIA Concepts

Cyber Crime Terms and Vocabulary

27000 Series Framework

Due Care and Due Diligence

Inside Threats and Ethics

Policies Start with Senior Management

Defining Risk

Control Types

Compliance Requirements

DR, BC, and BIA

Security Awareness Training

Intellectual Property and Licensing

Policy Life Cycle

Threat Modeling

Supply Chain Risk Management

Information Security: Asset Security

Overview

Classifying Assets and Information

Stewards and Custodians of Assets and Information

Protecting Privacy

Data Retention

Determining Security Controls

Data State and Resources for Security Control Frameworks

Information and Asset Handling Policies

Security Crime Investigations and the Data lifecycle

Overview

Types of Investigations

Evidence and the Investigation Process

Types of Computer Crimes

ISC2 Code of Ethics

Asset Management

Data Roles

WEEK 2

Managing the Data Lifecycle

Information Security: Security Architecture and Engineering

Overview

Designing with Security in Mind

Security Model Fundamentals

System Security Requirements

Hardware and Firmware Security Capabilities

Assessing Vulnerabilities

Vulnerabilities in Web-Based Systems

Vulnerabilities in Mobile Systems

Vulnerabilities in Embedded Devices

Facility Design and Controls

Symmetric Encryption Concepts

Symmetric Keys and Algorithms

Asymmetric Encryption Concepts

Digital Signature Concepts

Hashing for Integrity

Asymmetrical Encryption with Email

PKI and Revoking Certificates

Power Considerations

Information Security: Communication and Network Security

Overview

OSI and IP Models

IP Networking

Wi-Fi Security Considerations

Network Component Security

Virtualized Network Security Considerations

Securing Communications Channels

Security Design and Attacks

Overview

Secure Design Principals

WEEK 3

Assess and Mitigate Vulnerabilities

Cryptanalytic Attacks

Resiliency Technologies

Communications and Network Security

Information Security: Identity and Access Management (IAM)

Overview

Identity Management (IdM)

AAA as Part of Our Controls

Centralized Authentication with RADIUS

Using LDAP with Directory Services

Multi-Factor Authentication Categories

Biometric Acceptance and Rejection Rates

Options for Biometric Authentication

DAC, MAC, and RBAC

IAM Provisioning Lifecycle

Information Security: Security Assessment and Testing

Overview

Testing, Auditing, and Assessment Overview

Penetration Testing

Vulnerability Scans and Assessments

Reviewing and Testing Code

Security-Related Data Collection

Continuous Monitoring

Information Security: Security Operations

Overview

Supporting Investigations

Types of Evidence

Chain of Custody

Forensics Process

WEEK 4

Separation of Duties

Media Management

Backups

Logging with Separation of Duties

RAID Concepts

Incident Response Overview

Phases of Incident Handling

Improving Security with Configuration Management

Patch Management

Change Management

Comparing IDS and IPS

IDS and IPS Detection Methods

Network vs Host-Based IDS and IPS

IDS and IPS Alarms

Traditional and Next-Generation Firewalls

Categorizing Vulnerabilities with CVSS

Calculating Vulnerability Scores

Honeypots

Fault Tolerance for Availability

DR and Alternate Sites

H/W and S/W Planning for DR

Directing and Communicating DR

Personnel Safety and Security

Information Security: Software Development Security

Overview

Software Development Security

Software Development Life Cycle (SDLC)

Change Management

Software Capability Maturity Model (CMMI)

Programming Concepts

Programming Methodology

WEEK 5

Common Software Vulnerabilities

Web Software Vulnerabilities

Security Controls and Development

Overview

Identity and Access Management (IAM)

Security Assessment and Testing

Security Operations

Managing Threats

Development Methodologies and Maturity Models

Securing Development Environments

Software Security

Last updated 1.12.2026