Certified Information Systems Security Professional (CISSP) Review Bootcamp

Course CISSP-E 5 Days Instructor-led, Hands on

Introduction

CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 9th Edition has been completely updated for the latest 2021 CISSP Body of Knowledge. You'll prepare for the exam smarter and faster thanks to expert content, real-world examples, advice on passing each section of the exam, access to the Sybex online interactive learning environment, and much more. Reinforce what you've learned with key topic exam essentials and chapter review questions.

**For those looking to take the exam, this course is a great review for all the domains. You should not assume that you will be ready to take this particular exam just by attending this class.

**Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention. View the full list of supplementary references at www.isc2.org/certifications/References.

Prerequisites

This course is intended for professionals with at least 5 years of recent, full-time professional work experience in 2 or more of the above 8 domains.

Candidates for the exam must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK. Earning a four-year college degree or regional equivalent or an additional credential from the (ISC)² approved list will satisfy one year of the required experience. Education credit will only satisfy one year of experience.

A candidate who doesn't have the required experience to become a CISSP may become an Associate of (ISC)² by successfully passing the CISSP examination. The Associate of (ISC)² will then have six years to earn the five years required experience.

Work Experience:

Your work experience must fall within two or more of the eight domains of the (ISC)² CISSP CBK:

- Domain 1. Security and Risk Management

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Domain 2. Asset Security
- Domain 3. Security Architecture and Engineering
- Domain 4. Communication and Network Security
- Domain 5. Identity and Access Management (IAM)
- Domain 6. Security Assessment and Testing
- Domain 7. Security Operations
- Domain 8. Software Development Security

Full-Time Experience: Your work experience is accrued monthly. Thus, you must have worked a minimum of 35 hours/week for four weeks in order to accrue one month of work experience.

Part-Time Experience: Your part-time experience cannot be less than 20 hours a week and no more than 34 hours a week.

- 1040 hours of part-time = 6 months of full time experience
- 2080 hours of part-time = 12 months of full time experience

Internship: Paid or unpaid internship is acceptable. You will need documentation on company/organization letterhead confirming your position as an intern. If you are interning at a school, the document can be on the registrar's stationery.

Objectives:

This course covers 100% of all exam objectives including:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Course Materials

Each student will receive an exam review guide.

Course Outline

Module 1: Security and Risk Management

- Understand, adhere to, and promote professional ethics
- Understand and apply security concepts
- Evaluate and apply security governance principles
- Determine compliance and other requirements

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Understand legal and regulatory issues that pertain to information security in a holistic context
- Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply Supply Chain Risk Management (SCRM) concepts
- Establish and maintain a security awareness, education, and training program

Module 2: Asset Security

- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision resources securely
- Manage data lifecycle
- Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
- Determine data security controls and compliance requirements

Module 3: Security Architecture and Engineering

- Research, implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
- Select controls based upon systems security requirements
- Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security
- architectures, designs, and solution elements
- Select and determine cryptographic solutions
- Understand methods of cryptanalytic attacks
- Apply security principles to site and facility design
- Design site and facility security controls

Module 4: Communication and Network Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Module 5: Identity and Access Management

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

Module 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate report
- Conduct or facilitate security audits

Module 7: Security Operations

- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management
- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Module 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in software development ecosystems
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure code