THINQTANK® LEARNING

(ISC)² CISSP
Certified Information Systems Security Professional

Our Learning Exclusive

- Custom exam prep software and materials
- Course specific thinQtank® Learning publications to promote fun exciting learning
- Extended hours of training with deeper dives into technical domains
- WE DO NOT "TEACH THE TEST" We always deliver valuable example and discussion
- Receive all reading material and study guides when you register
- All courses taught by CISSP expert instructors

Course Duration

- Seven days of instructor-led training
- Intensive deep-dive lessons on all eight domains

Prerequisites

- Professionals with at least five years of experience and who demonstrate a globally recognized level of competence, as defined in the CISSP Common Body of Knowledge (CBK) in two or more of the eight security domains

Target Audience

- Anyone whose position requires CISSP Certification
- Individuals who want to advance within their current computer security careers or migrate to a related career

Exam Information

- (ISC)2 CISSP Exam

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive for Certification Success

- Course materials are constantly updated to reflect the latest changes in the CISSP Certification Exam
- CISSP course now includes prep and review for the new CISSP visual exam question format (both Drag and Drop and Hotspot)
- CISSP preparation includes certification exam through drill sessions, review of the entire Common Body of Knowledge, and practical question and answer scenarios.
- Digital courseware for 24/7 access to authorized course materials, including changes and updates
- **Retake the class as many times as you like for 24 months – online or in person**

Course Overview

thinQtank® Learning is offering an industry unique seven-day training camp in which students can receive the (ISC)2 CISSP certification training. Our 7-Day CISSP training course is the best things you can do to prepare yourself to pass the CISSP exam. The CISSP certification is an elite way to demonstrate your knowledge, advance your career and become a member of a community of cybersecurity leaders. It shows you have all it takes to design, engineer, implement and run an information security program.

This course is the most comprehensive review of information security concepts and industry best practices, and covers the eight domains of the official CISSP CBK (Common Body of Knowledge). You will gain knowledge in information security that will increase your ability to successfully implement and manage security programs in any organization or government entity. You will learn how to determine who or what may have altered data or system information, potentially affecting the integrity of those asset and match an entity, such as a person or a computer system, with the actions that entity takes against valuable assets, allowing organizations to have a better understanding of the state of their security posture. Policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets are also covered in this course.

This seven-day program is comprised of a total of eight domains:

- Official (ISC)2 Guide to the CISSP Common Body of Knowledge® (CBK) (Kindle Edition) (Optional)
- CISSP Comprehensive Review Notes 2016 (Kindle Edition) (Optional)
- Updated (ISC)2 CISSP Flash Cards
- CISSP Practice Test Questions
- CISSP Certification Exam Voucher (Optional)
- Updated CISSP Domain Review and Cheat Sheet

Course Objectives

In-depth coverage of the eight domains required to pass the CISSP exam:

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

THINQTANK® LEARNING

(ISC)² CISSP
Certified Information Systems Security Professional

Course Modules

1 Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity)
- Understand and Apply Concepts of Confidentiality, Integrity, and Availability
- Apply Security Governance Principles
- Compliance
- Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
- Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines
- Understand Business Continuity Requirements
- Contribute to Personnel Security Policies
- Understand and Apply Risk Management Concepts
- Understand and Apply Threat Modeling
- Integrate Security Risk Considerations into Acquisitions Strategy and Practice
- Establish and Manage Security Education, Training, and Awareness

2 Asset Security (Protecting Security of Assets)
- Classify Information and Supporting Assets
- Determine and Maintain Ownership
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Establish Handling Requirements

3 Security Engineering (Engineering and Management of Security)
- Implement and Manage an Engineering Life Cycle Using Security Design Principles
- Understand Fundamental Concepts of Security Models
- Select Controls and Countermeasures Based Upon Information Systems Security Standards
- Understand the Security Capabilities of Information Systems
- Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
- Assess and Mitigate Vulnerabilities in Web-based Systems
- Assess and Mitigate Vulnerabilities in Mobile Systems
- Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems
- Apply Cryptography
- Apply Secure Principles to Site and Facility Design
- Design and Implement Facility Security

4 Communications and Network Security (Designing and Protecting Network Security)
- Apply Secure Design Principles to Network Architecture
- Securing Network Components
- Design and Establish Secure Communication Channels
- Prevent or Mitigate Network Attacks

5 Identity and Access Management (Controlling Access and Managing Identity)
- Control Physical and Logical Access to Assets
- Manage Identification and Authentication of People and Devices
- Integrate Identity as a Service (IDaaS)
- Integrate Third-Party Identity Services
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Manage the Identity and Access Provisioning Life Cycle

(ISC)² CISSP
Certified Information Systems Security Professional

Course Modules Continued

6 Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

- Design and Validate Assessment and Test Strategies
- Conduct Security Control Testing
- Collect Security Process Data
- Conduct or Facilitate Internal and Third-Party Audits

7 Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

- Understand and Support Investigations
- Understand Requirements for Investigation Types
- Conduct Logging and Monitoring Activities
- Secure the Provisioning of Resources through Configuration Management
- Understand and Apply Foundational Security Operations Concepts
- Employ Resource Protection Techniques
- Conduct Incident Response
- Operate and Maintain Preventative Measures
- Implement and Support Patch and Vulnerability Management
- Participate in and Understand Change Management Processes
- Implement Recovery Strategies
- Implement Disaster Recovery Processes
- Test Disaster Recovery Plan
- Participate in Business Continuity Planning
- Implement and Manage Physical Security
- Participate in Personnel Safety

8 Software Development Security

(ISC)² CISSP
Certified Information Systems Security Professional

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com