# Certified Information Systems Security Professional (CISSP)

## Overview

This Official (ISC)² course provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of the CISSP: Security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security. In this course, you will find that several types of activities are used to reinforce topics and increase knowledge retention. These activities include open-ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

## Audience

This training course is intended for professionals who have at least 5 years of recent full-time professional work experience in 2 or more of the 8 domains of the CISSP CBK and are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current information security careers. This course is ideal for those working in positions such as, but not limited to:

- Security consultant
- Security manager
- IT director/manager
- Security auditor
- Security architect
- Security analyst
- Security systems engineer
- Chief information security officer
- Director of security
- Network architect

## Course objectives

- Understand and apply the concepts of risk assessment, risk analysis, data classification, and security awareness, and implement risk management and the principles used to support it (risk avoidance, risk acceptance, risk mitigation, risk transference)
- Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization’s security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization’s core goals and strategic direction and address the frameworks and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets, as well as to assess the effectiveness of that protection and establish the foundation of a comprehensive and proactive security program to ensure the protection of an organization’s information assets
- Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization’s security processes, information security systems,

personnel, and organizational sub-units so that these practices and processes align with the organization’s core goals and strategic direction and examine the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality, and authenticity
- Understand the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media, and identify risks that can be quantitatively and qualitatively measured to support the building of business cases to drive proactive security in the enterprise
- Offer greater visibility into determining 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
- Plan for technology development, including risk, evaluate the system design against mission requirements, and identify where competitive prototyping and other evaluation techniques fit in the process
- Protect and control information-processing assets in centralized and distributed environments and execute the daily tasks required to keep security services operating reliably and efficiently
- Understand the Software Development Life Cycle (SDLC) and how to apply security to it, and identify which security control(s) are appropriate for the development environment, and assess the effectiveness of software security

## Benefits to you

This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam and features:

- Official (ISO)2 courseware
- Taught by an authorized (ISC)2 instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

## Course Outline

Domain 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
- Understand professionals ethics
- Develop and implement documented security policy, standards and 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 acquisition strategy and practice
- Establish and manage information security education, training, and awareness

Domain 2: Asset security (Protecting security of assets)

- Classify information and supporting assets (e.g., sensitivity, criticality)
- Determine and maintain ownership (e.g., data owners, system owners, business/mission owners)
- Protect privacy
- Ensure appropriate retention (e.g., media, hardware, personnel)
- Determine data security controls (e.g., data at rest, data in transit)
- Establish handing requirements (marketing, labels, storage, and destruction of sensitive information)

Domain 3: Security engineering (Engineering and management of security)

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models (e.g., confidentiality, integrity, and multi-level models)
- Select controls and countermeasures based upon systems security evaluation models
- Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module, interfaces, fault tolerance)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Assess and mitigate vulnerabilities in web-based systems (e.g., XML, OWASP)
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems (e.g., network-enabled devices, Internet of things [loT])
- Apply cryptography
- Apply secure principles to site and facility design
- Design and implement physical security

Domain 4: Communications and network security (Designing and protecting network security)

- Apply secure design principles to network architecture (e.g., IP and non-IP protocols, segmentation)
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

Domain 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 identify as a service (e.g., cloud identity)
- Integrate third-party identity services (e.g., on-premise)
- Implement and manage authorization mechanisms

- Prevent or mitigate access control attacks
- Manage the identity and access provisioning lifecycle (e.g., provisioning, review)

Domain 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 (e.g., management and operational controls)
- Analyze and report test outputs (e.g., automated, manual) Conductor facilitate internal and third party audits

Domain 7: Security operations (e.g., foundational concepts, investigations, incident management, disaster recovery)

- Understand and support investigations
- Understand requirements for investigations types
- Conduct logging and monitoring activities
- Secure the provisioning of resources
- Understand and apply foundational security operations concepts
- Employ resource protection techniques
- Conduct incident management
- Operate and maintain preventative measures
- Implement and support patch and vulnerability management
- Participate in and understand change management processes (e.g., versioning, baselining, security impact analysis)
- Implement recovery strategies
- Implement disaster recovery processes
- Test disaster recovery plans
- Participate in business continuity planning and exercises
- Implement and manage physical security
- Participate in addressing personnel safety concerns (e.g., duress, travel, monitoring)

Domain 8: Software development security (Understanding, applying, and enforcing software security)

- Understand and apply security in the software development lifecycle
- Enforce security controls in development environment
- Assess the effectiveness of software security
- Assess security impact of acquired software