CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

Syllabus

Course Title: Certified Information Systems Security Professional
Course Length: 32 hours
Instructor: Mahesh Kumawat
Course Type: Offline Class

Course Description: The CISSP certification from ISC2 is one of the premier certifications in the Information Security industry. Covering numerous topics across 8 Domains, this certification speaks to a well-rounded understanding of the many facets of protecting organizational assets. Designed around eight specific domains, this course examines : Security & Risk Management , Asset Security, Security Architecture and Engineering, Communication & Network Security, Identity & Access management , Security Assessment & Testing,, Security Operations and Software Development Security.

Why should I take this course? : The CISSP certification is the gold standard for information systems security across the world. There are more than 140,000 professionals worldwide with the CISSP certification. The certification admits its holder to an exclusive club of information systems security professionals, cutting across industries and geographies.
Go to job portals anywhere in the world and type CISSP in the search box, and you will see for yourself the standing this certification has in the information security industry.
The CISSP certification helps you obtain an increase in salary and the breadth of content covered on the CISSP exam will benefit you and your organization.

Who is this for? : CISO, CIO, Director/Manager of Security, Security Auditor, Security Architect, and Security Consultant.

Prerequisites: To earn this certification, you must pass the exam as well as have 5 years of paid experience in two or more domains of the CISSP Common Body of Knowledge. However, if you have passed the examination but are short of the requisite experience, you can become an Associate of (ISC)^2. Thereafter, you will have 6 years' to earn the requisite experience.

Supplementary Materials: None as of now, may be provided throughout the course.

Sessions Overview: The entire program will be taught in 16 session of 2 hours each, or a total of 32 hours. Each of the eight domains will be covered in 2 sessions of 2 hours each, with allowance for some flexibility in the time earmarked for each domain.

Introduction (15 minutes):

- Introduction to CISSP and the eight domains in the Common Body of Knowledge (CBK)
- Examination pattern and Computerized Adaptive Testing (CAT)
- Certification process; partial waiver of work experience for candidates with college degrees.
- Sample questions to give candidates a feel of the examination.

Session 1 (1.75 hours): Domain 1: Security & Risk Management

- Confidentiality, integrity and availability
- Information security governance
- Compliance
- Legal and regulatory issues
- Professional ethics
- Policy, procedures, standards and guidelines

Session 2 (2 hours): Domain 1: Security & Risk Management

- Business continuity
- Personnel security policies and procedures
- Risk management concepts
- Threat modelling concepts
- Applying risk management to the supply chain
- Security awareness, training and education

Session 3 (2 hours): Domain 2: Asset Security

- Identify & classify information assets
- Information and asset ownership
- Privacy

Session 4 (2 hours): Domain 2: Asset Security

Asset retention

- **Data security controls**
- **Information and asset handling requirements**

Session 5 (2 hours): Domain 3: Security Architecture & Engineering

- Secure design principles
- Fundamental concepts of security models
- Controls based on system security requirements
- Security capabilities of information systems
- Vulnerabilities of security architectures

Session 6 (2 hours): Domain 3: Security Architecture & Engineering

- Vulnerabilities in web-based systems
- Vulnerabilities in mobile systems
- Vulnerabilities in embedded devices
- Cryptography
- Security in site and facility design
- Site and facility security controls

Session 7 (2 hours): Domain 4: Communication & Network Security

- Secure design principles in network architecture

Session 8 (2 hours): Domain 4:Communication & Network Security

- Secure network components
- Secure communication channels

Session 9 (2 hours): Domain 5: Identity & Access Management

- We will test secure network architecture design and secure network components in practice.
- Logical and physical access controls
- Identification and authentication of people, devices and services
- Identity as a service

Session 10 (2 hours): Domain 5: Identity & Access Management

- Authorization mechanisms
- I & A provisioning lifecycle

We will develop concepts on secure communication channels and network attacks.

Session 11 (2 hours): Domain 6: Security Assessment & Testing

- Design and validation of assessment, test and audit strategies
- Security control testing
- Collect security process data

Session 12 (2 hours): Domain 6: Security Assessment & Testing

We will develop ideas on about identity as a service, third party identity services, access control hacks and provisioning lifecycles.

- Analyzing test output and reporting
- Security audits

Session 13 (2 hours): Domain 7: Security Operations

We will explain security assessment and test strategies, security process data and security control testing.

- Understanding and supporting investigations
- Investigation requirements
- Logging and monitoring activities
- Securely provisioning resources
- Security operations concepts
- Resource protection techniques
- Incident management

Session 14 (2 hours): Domain 7: Security Operations

We will learn about test outputs and security architecture vulnerabilities.

- Detective and preventive measures
- Patch and vulnerability management
- Change management
- Recovery strategies
- DR process
- Testing DR plans
- BCP
- Physical security
- Personnel safety and security

Session 15 (2 hours): Domain 8: Software Development Security

We will learn about investigations support and requirements, logging and monitoring activities, provisioning of resources, foundational security operations concepts , resource protection techniques and incident management,

- Integrating security in SDLC
- Security controls in development environments
- Effectiveness of software security

<u>Session 16 (2 hours):Domain 8: Software Development Security</u>

We will summarize concepts such as preventive measures, patch and vulnerability management, changing management processes, recovery strategies, disaster recovery processes and plans, business continuity planning and exercises and physical security.

- Security impact of acquired software
- Secure coding guidelines and security

SESSIONS CALENDAR

Date, Time (IST)	**Session ID**
	Session 1 : Security and Risk Management Part 1
	Session 2: Security and Risk Management Part 2
	Session 3 : Asset Security Part 2
	Session 4: Asset Security Part 2
	Session 5: Security Engineering Part 1
	Session 6: Security Engineering Part 2
	Session 7: Communication and Network Security Part 1
	Session 8: Communication and Network Security Part 2
	Session 9: Identity and Access Management Part 1
	Session 10: Identity and Access Management Part 2
	Session 11 : Security Assessment and Testing
	Session 12: Security Assessment and Testing Part 2
	Session 13: Security Operations Part 1

	Session 14: Security Operations Part 2
	Session 15: Software Development Security Part 1
	Session 16: Software Development Security Part 2