Certified Information Systems Security Professional (CISSP)

Gain and Understand the best practices to work on the forefront in Information Security Domain.

Exam and Course Outline

CODEC Networks Pvt Ltd

507, New Delhi House, Barakhamba Road, New Delhi 110001 trainings@codecnetworks.com
+91 11 43752299, 9971676124

Course Overview

Certified Information Systems Security Professional (CISSP) is a registered trademark and course developed by (ISC)² and the most globally recognized certification in the information security market.

CCSP course and certification exam ensure professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

Backed by (ISC)², the globally recognized not-for-profit organization dedicated to advancing the cyber, information, software, and infrastructure security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024.

The course is designed purposely to give participants an idea to decide how valuable the CISSP is, and understand to attain the certification.

This course is based on guidelines to cover the below following topics / domains and provide participants a curve in there preparation of CISSP Exam.

Domain 1 - Security and Risk Management
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

This preparation course focuses and develops expertise in defining IT Security best practices in designing, building, managing, architecting, maintaining and controlling a secure business environment.

By attending this course, professionals will get a comprehensive review of the knowledge and skills required across security policy development and management, as well as a technical understanding of a wide range of security controls.

Upon successful passing the CISSP Exam, professional will gain the skills and knowledge necessary to:

- 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.
- Apply a comprehensive and rigorous method for describing a current and/or future structure and behaviour 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 to
  - 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
  - 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 and 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

Who Should Attend

This program is intended for professionals who have at least 5 years of in Information Systems and Security domain. The program is ideal for those working in positions such as, but not limited to -

- Security Consultant/Manager, IT Director/Manager, Security Auditor/Architect/Analyst/ Systems Engineer, Chief Information Security Officer or Director of Security

Course Duration

40 Hours (5 Days * 8 Hours)

Course Content / Outline

Domain 1 - Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles
- Determine compliance requirements
- Understand legal and regulatory issues that pertain to information security in a global context
- Understand, adhere to, and promote professional ethics
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC)
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education, and training program

Domain 2 - Asset Security

- Identify and classify information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

Domain 3 - Security Architecture and Engineering

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based upon systems security requirements
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- 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
- Apply cryptography
- Apply security principles to site and facility design
- Implement site and facility security controls

Domain 4 - Communication and Network Security

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

Domain 5 - Identity and Access Management (IAM)

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

Domain 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

Domain 7 - Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Securely provisioning resources
- Understand and apply foundational security operations concepts
- Apply resource protection techniques
- 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

Domain 8 - Software Development Security

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