CISSP Training Course

CISSP®

Certified
Information
Systems Security
Professional

Overview

Certified Information Systems Security Professional (CISSP) is one of the world's premier cybersecurity certifications offered for professionals worldwide. This CISSP certification course is ideal for professionals who are looking to demonstrate their knowledge across different security practices and principles. This 5-day Certified Information Systems Security Professional (CISSP) certification is governed by the not-for-profit International Information Systems Security Certification Consortium (ISC)2.

CISSP is the most renowned certification in the information security domain. Our CISSP certification training program aims to equip participants with in-demand technical and administrative competence to design, architect, and manage an organization's security posture by applying internationally accepted information security standards. The training offers an in-depth understanding of eight domains that comprise CISSP common body knowledge (CBK) and prepares you for the CISSP exam held by the (ISC)^2.

(ISC)^2 is a globally recognized, non-profit organization dedicated to advancing the information security field. The CISSP was the first credential in information security to meet the stringent requirements of ISO/IEC Standard 17024. It is looked upon as an objective measure of excellence and a highly reputed standard of achievement.

CISSP Training

The Certified Information Systems Security Professional Certification course from ISC2 is one of the most sought-after certification courses in the Cybersecurity domain. There is an increase in security breaches on a daily basis irrespective of the size of an organization. Be it SMBs, Large MNCs, or Government Institutions, hacking, malware, phishing is completely tarnishing the image of the company, and business-critical data is no more secure.

CISSP Certification was clearly developed to address these cybersecurity threats and provide a secure environment by using widely-recognized information security standards. Participants taking part in this CISSP training will get a copy of the course material that is completely aligned with ISC2 CISSP Common Body of Knowledge and will receive a course completion certificate from an ISC2 Official Training Provider.

Learning Objectives

Participants who take part in the Certified Information Systems Security Professional (CISSP) training will learn about:

- A holistic understanding of information security aspects in an organization
- Defining the architecture, design, and management of IT security
- Necessary skills required to become a CISSP certified professional
- Gain a thorough understanding of all the Eight domains prescribed in the ISC2 CISSP Common Body of Knowledge (CBK)
- Optimizing security operations in an enterprise
- Access control systems and various methodologies that complement IT Security and governance for an enterprise.

Skills Measured/CISSP Examination Weights

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

Domain 1: Security and Risk Management

- Applying the concepts of confidentiality, integrity and availability
- Evaluating and applying security governance principles
- Determining compliance requirements
- Understanding the legal and regulatory issues related to information security
- Understanding, adhering to, and promote professional ethics
- Developing, documenting, and implementing security policies and guidelines
- Understanding Business Continuity (BC) requirements
- Contributing personnel security policies and procedures
- Applying risk management concepts
- Applying threat modelling concepts and methodologies
- Applying risk-based management concepts to the supply chain
- To establish and maintain security awareness, education, and training program across the organization

Domain 2: Asset Security

- Identifying and classifying information and assets
- Determining and maintaining information and asset ownership
- Protecting privacy
- Ensuring appropriate asset retention
- Determine data security controls
- Establishing information and asset handling requirements

Domain 3: Security Architecture and Engineering

- Implementing engineering processes by using secure design principles
- Understanding the fundamental concepts of security models
- Selecting controls based upon systems security requirements
- Understanding security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assessing and mitigating vulnerabilities of security architectures, solution elements, and designs
- Assessing and mitigating vulnerabilities in web-based systems
- Assessing and mitigating vulnerabilities in mobile systems
- Assessing and mitigating vulnerabilities in embedded devices
- Applying cryptography
- Implementing site and facility security controls

Domain 4: Communication and Network Security

- Implementing secure design principles in network architectures
- Securing network components
- Implementing secure communication channels according to design

Domain 5: Identity and Access Management (IAM)
Domain 6: Security Assessment and Testing
Domain 7: Security Operations
Domain 8: Software Development Security