Wissenhive

CISSP Training Certification

Table of Contents

About the Program

This program is one of the globally recognized certifications that will help apprentices prepare for the Certified Information Systems Security Professional examination by providing the foundational knowledge required to plan and define architecture effectively for building, designing, managing, engineering, and leading an organization's security postures.

Wissenhive's CISSP certification training programs are professionally designed to cover topics in detail, including Cryptography, accessing control systems, and practicing the management of security by covering eight information system security domains. Masters in understanding security models & architecture, Cryptography, networking & telecommunications security, investigation, law & ethics, accessing control methodology and systems, and so on.

Key Training Features

- Ask Questions Real-Time and Interact with the Trainer Live
- Learner assistance and support - 24x7x365
- Flexible classes
- High-quality content created by industry experts
- Professionally designed Student Training Material
- High-Quality Audio-Video Lectures
- Lifetime Training Access
- Assessments

CISSP®

Training Options

- Self-paced Training
- Live Virtual Classes
- One on One Training

Why Java?

- Higher Paying Opportunities
- Gain Knowledge and Credibility
- Stand Out Among the Ordinary
- Knowledge of CISSP Best Practices
- Better Career Growth & Job Opportunities
- Better ROI with Flexibility
- Sharpen your IT Skillset

CISSP®

What will you learn?

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

CISSP®

Career Option with Salary Compensation

Security Administrator

- Minimum - $49,000
- Avg Salary - $67,000
- Maximum - $94,000

Security Consultant

- Minimum - $60,000
- Avg Salary - $88,000
- Maximum - $138,000

Security Analyst

- Minimum - $53,000
- Avg Salary - $74,000
- Maximum - $116,000

Security Engineer

- Minimum - $62,000
- Avg Salary - $93,000
- Maximum - $135,000

Security Specialist

- Minimum - $60,000
- Avg Salary - $72,000
- Maximum - $87,000

CISSP®

Target Audience

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

Prerequisites

There are prerequisites for taking the CISSP (Certified Information Systems Security Professional) Certification; Wissenhive recommends having

- Minimum 5 years of cumulative paid working experience in 2 or more of the 8 domains of the CISSP® Common Body of Knowledge
- 1 year experience waiver can be a four-year college degree, or regional equivalent, or additional cre dential from the (ISC)² approved list

CISSP®

Course Content

- Developing, documenting, and implementing security standards, policies, guidelines, and procedures.
- Identifying and classifying assets and information
- Managing and maintaining data lifecycle
- Selecting and determining cryptographic solutions
- Assessing and implementing the security design principles in network architectures
- Completing incident management
- Assessing and mitigating the vulnerabilities of security designs, architectures, and solution elements
- Managing and maintaining identification and authentication of devices, people, and services
- Complete logging and monitoring activities
- Completing the security control testing
- Maintaining and operating preventive and detective measures
- Understanding and integrating security in the SDLC (Software Development Life Cycle)

CISSP®

Course Curriculum:

1. **Indepth understanding of Information Systems Security**

2. **Security and Risk Management**

- Understanding adhere to, and promotion of professional ethics
- Understanding and Applying Security Concepts
- Evaluatating and Applying Security Governance Principles
- Control Frameworks, Due Diligence and Due Care
- Legal and Regulatory Issue
- Intellectual Properties (IP) Law Types
- OECD Principles, GDPR, Data Protection Principles, and Data Protection principles
- Developing, Documenting, and Implementing Security Policy
- Business Continuity Planning Phases and Business Impact Analysis
- Risk Analysis: Introduction and Assessment
- Security Control Assessment
- Risk Monitoring and Continuous Improvement
- Risk Handling and Security Control Assessment

3. **Asset Security**

- Asset Security: identification and classification
- Establishing Information and Asseting Handling Requirements
- Data Life Cycle: Built, Store, Use, Share, Archive, and Destroy
- Data Remanence and Data Destruction
- Data Loss Prevention (DLP) and Digital Rights Management (DRM)

CISSP®

Course Curriculum:

4. **Security Architecture and Engineering**

- Introduction to Security Engineering
- Researching, Implementing, and Managing Engineering Processes
- Understanding the Fundamental Concepts of Security Models
- Security Models Types
- Security Capabilities of Information Systems
- Security Concerns of ICS
- SCADA
- Cloud Computing
- Internet of Things
- Selecting and Determining Cryptographic Solutions
- Data Encryption Standards, Encryption Methods, and Cryptosystem Elements
- Designing Site and Facility Security Controls
- Asymmetric Cryptography, Advanced Encryption Standards, and Public Key Infrastructure
- Hashing, MAC, and Digital Signatures
- Applying Security Principles to Site and Facility Design
- Environmental Security Controls and Personnel Access Controls
- HVAC, Power Supply, and Training

CISSP®

Course Curriculum:

5. **Communications and Network Security**

- Physical Layer and Data Link Layer
- Assess and Implement Secure Design Principles
- Layer: Physical, Data Link, Transport, Network, Presentation, Session, and Application
- IPv6 and Its Address Structures
- Protocol: Internet Security Protocol, Secure Security Protocol, IPsec Security Protocols
- Secure Network Components
- Implementing Secure Communication Channels
- VPN Protocols

6. **Identity and Access Management**

- Identity and Access Management: Introduction, Controlling, and Managing
- Biometrics and Accuracy Measurement
- Tokens, Token Devices, and Authorization
- Passwords and Its Types
- Federated Identity Management (FIM) and Credential Management System
- Federated Identity with a Third-Party Service
- Implementing and Managing Authorization Mechanisms
- Implement Authentication Systems
- Managing the Identity and Access Provisioning Life Cycle
- Kerberos and Its Steps, RADIUS, TACACS, and TACACS Plus

CISSP®

Course Curriculum:

7. **Security Assessment and Testing**

- Designing and Validatating Assessment, Test, and Audit Strategies
- Internal Audit, External Audit, Third-party Audit and Assessment
- Penetration Testing Process and Testing Types
- Log Management
- Testing and Interface Methods
- Analyzing Test Output and Generate Report

8. **Security Operations**

- Understanding and Complying with Investigations
- Digital Forensics
- Digital Forensics Tools, Tactics, Procedures, and Artifacts
- Conduct Logging, Continuous Monitoring, and Monitoring Activities
- Perform and identifying Conduct Incident, Configuration and Access Management
- Apply Resource Protection
- Operating and Maintaining Preventive and Detective Measures
- Understand Anti-Malware Systems, Deep Learning, Machine Learning, and AI
- Implementing and Support Vulnerability and Patch Management
- Implementing and recovering with effective Recovery Strategies
- Implement Disaster Recovery (DR) Processes
- Test Disaster Recovery Plans (DRP) and Business Continuity (BC)
- Importance of Lighting in Security Management
- Address Personnel Safety and Security Concerns

CISSP®

Course Curriculum:

9. **Software Development Security**

- Integrating Security in the Software Development Life Cycle
- Extreme and Software Programming Model
- CMM and SAMM
- DevOps and DevSecOps
- Change Management and Integrated Product Team (IPT)
- Software Development Ecosystems
- Software Configuration Management
- Assessing Security Impact of Acquired Software
- Free and Open Source Software
- Database and Data Warehousing Environments
- Defining and Applying Secure Coding Guidelines and Standards

CISSP®

Contact us

DREAM BIG IT SOLUTION INDIA PVT LTD

Noida

B-115, B Block, Sector 2,
Noida, Uttar Pradesh-201301

If you have any further questions or would like to chat with us, give us a call

IND +91 9368569359 **US** +1 (908)-(952)-(2400)

https://www.facebook.com/Wissenhive

https://www.linkedin.com/company/wissenhive/

https://www.instagram.com/wissenhive/

https://twitter.com/HiveWissen

https://in.pinterest.com/wissenhive/

https://www.youtube.com/channel/UCEaIUuf4czgsl9F0PTs0lDg

CISSP®