

CISSP® TRAINING

EXAM PREPARATION TRAINING

WISELEARNER

WHAT IS CISSP?

- Accelerate your cyber security career with the CISSP certification.
- Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cyber security program. With a CISSP, you validate your expertise and become an $(ISC)^2$ member, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.
- Prove your skills, advance your career, and gain the support of a community of cyber security leaders here to support you throughout your career.
- The Certified Information Systems Security Professional (CISSP) exam is designed to ensure that someone handling computer security for a company or client has mastered a standardized body of knowledge.

BENEFIT OF CISSP

- Protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure business environment
- Increase confidence that candidates are qualified and committed to information security
- Ensure employees use a universal language, circumventing ambiguity with industry-accepted terms and practices
- Increase organizations' credibility when working with clients and vendors
- According to $(ISC)^2$, increasing regulatory compliance within the public and private sectors requires strong security policies, processes, and controls, which force organizations to adopt security standards and frameworks for a long-term approach to mitigating risk.



WHO SHOULD ATTEND?

- 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

LEARNING 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
- 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, 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
- Apply a comprehensive and rigorous method for describing a current and 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



COURSE CONTENTS

Overview of CISSP & Certification Exam

Domain 1: Security and Risk Management

- Confidentiality, integrity and availability
- Security governance principles
- Compliance
- Legal and regulatory Issues
- Ethics
- Business continuity requirements
- Policies, standards, procedures, and guidelines
- Risk management concepts
- Threat modelling
- Education, training, and awareness

Domain 2: Asset Security

- Data classification
- Data owners
- System owners
- Business/Mission owners
- Privacy
- Data processors
- Data remanence
- Limitation on collection of sensitive data
- Data retention
- Data destruction
- Baselines
- Scoping and Tailoring

Domain 3: Security Engineering

- Secure design principles
- Security models
- Controls and counter measures
- Virtualization
- Trusted platform module
- Applets
- Database security
- Cloud computing
- SCADA, XML
- OWASP
- The Internet of Things
- Cryptography, Symmetric, Asymmetric, Hash, PKI
- Digital signatures
- Non-repudiation
- Salts, Rainbow tables
- Cryptanalysis
- Facility design considerations
- Physical security
- Safety, Data center security
- Handling evidence, HVAC
- Fire prevention and suppression

Domain 4: Communication and Network Security

- Network architecture
- OSI model, TCP/IP
- Mutilayer protocols
- Storage protocols
- NAS, FCOE, iSCSI
- Voiceover IP
- Software-defined networks
- Wireless, 802.11
- WPA and WPA2
- Network devices
- Switches, Routers, Firewalls, Proxies
- Content distribution networks
- Remote meeting technology
- Telecomputing
- Remote access and VPN
- SSH, VPN, IPsec, SSL/TLS
- Port isolation, VLANs

Domain 5: Identity and Access Management

- Physical and logical access
- SSO, LDAP
- Multi-factor authentication
- Biometrics, Accountability
- Session management
- SAML, Credential management
- Third-party identity services
- Authorization mechanisms
- MAC, DAC, Rule-based, RBAC, Provisioning

Domain 6: Security Assessment

- Assessment and test strategies
- Security control testing
- Vulnerability assessment
- Penetration testing
- Log reviews
- Synthetic transactions
- Security testing strategies
- Security process
- Account management
- Management review
- Training and awareness
- Disaster recovery and business continuity
- Internal and third-party audits



COURSE CONTENTS

Domain 7: Security Operations

- Investigations
- Evidence collection and handling
- Reporting and documenting
- Forensics
- Operational, criminal, civil, and regulatory investigations
- eDiscovery
- Logging and monitoring
- Intrusion detection and prevention
- SIEM
- Continuous monitoring
- Egress monitoring
- Provisioning
- Asset inventory
- Configuration management
- Physical, virtual, and cloud assets
- SaaS
- Security operations
- Need-to-know and least privilege
- Service-level agreements
- Incident management
- Firewalls
- IDS and IPS
- Honeypots and honeynets
- Vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes
- Disaster recovery plans

Domain 8: Software Development Security

- Software development lifecycle
- Software development methodologies
- Waterfall
- Spiral
- Agile
- Software capability maturity models
- CMM
- Change management
- DevOps
- Security vulnerabilities
- Bounds checking
- Input/output validation
- Buffer overflow
- Privilege escalation
- Secure coding
- Code repositories
- Programming interfaces
- Assessing software security
- Black box testing
- White box testing
- Cramming
- Fuzzing

CERTIFICATION

CISSP CERTIFICATION EXAM INFORMATION	
Exam Length	3 Hours
Number of Questions	100 - 150
Question Format	Multiple Choice
Passing Grade	700 out of 1000
Testing Centre	PearsonVue Testing Centre
Exam Price	$ 699



PREREQUISITE

- Candidates must have a minimum of five years cumulative paid work experience in two or more of the eight domains of the CISSP CBK.
- Education credit will only satisfy one year of experience.
- A candidate who doesn't have the required experience to become a CISSP may become an Associate of $(ISC)^2$ by successfully passing the CISSP examination. The Associate of $(ISC)^2$ will then have six years to earn the five years required experience.

WISELEARNER