Certified Information Systems Security Professional

SprintzeaL
Empowering Professionals

ABOUT CISSP

CISSP (Certified Information Systems Security Professional) is a vendor-neutral information security certification demonstrating deep competence in designing, engineering and managing information security systems. It draws from an up-to-date, common body of knowledge which covers threats, technologies, regulations, standards and practices within information technology. The certification is provided by (ISC)² (International Information System Security Certification Consortium, Inc.), a globally recognised not-for-profit organisation dedicated to educating and certifying IT Security professionals around the world.

The course consists of five days of classroom-based training The exam is computer based and must be booked separately through (ISC)2® here.

CISSP is the premier certification for demonstrating expertise in information security design and management. It is vendor-neutral, globally recognised and meets the rigorous ISO/IEC 17024 International Standard, making it an objective measure of excellence in security.

COURSE AGENDA

SECURITY AND RISK MANAGEMENT:

- Confidentiality, integrity, and availability concepts
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethic
- Security policies, standards, procedures and guidelines

ASSET SECURITY:

- Information and asset classification
- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)

SECURITY ENGINEERING :

- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

COMMUNICATION AND NETWORK SECURITY:

- Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

IDENTITY AND ACCESS MANAGEMENT:

- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service (e.g. cloud identity)
- Access control attacks
- Identity and access provisioning lifecycle (e.g. provisioning review)

SECURITY ASSESSMENT AND TESTING:

- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architectures vulnerabilities

SECURITY OPERATIONS:

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

SOFTWARE DEVELOPMENT SECURITY:

- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact

PREREQUISITES :

CISSP is intended for security professionals with a minimum of either five years full-time paid work experience, or four years' experience, plus an information security university degree, in two or more of the following 8 CISSP domains:

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

Don't have the required experience? Not to worry. By passing the exam, you can become an Associate of (ISC) . You'll then have 6 years to gain the experience required to become a CISSP.

CISSP EXAM:

The exam tests knowledge in the 8 domains of CISSP
Multiple choice
6 hours
250 questions
Computer-based
Pass mark is a scaled score of 700/1000

BENEFITS::

FOR EMPLOYEES:

Helps you stand out in a competitive market of IT Security professionals
Indicates deep technical knowledge and skills
Shows commitment to the field of information security

FOR EMPLOYERS:

Ensures your information security staff are professionals with the expertise required to build and maintain an IT security program
Makes sure professionals are up to date with and able to protect against the latest threats

Provides your organisation with information security credibility when dealing with other companies or clients.

CONTACT US

INDIA

No 16, Zillion Biz Center
4th Block, Kormangala
Bangalore - 560034

USA

S Jones Blvd (304) #2014
LAS VEGAS
NV - 89107
USA

info@sprintzeal.com

080 6566 6771

315 675 7776