CISSP – certification Course

The CISSP training course covers topics such as Access Control Systems, Cryptography, and Security Management Practices, teaching students the eight domains of information system security knowledge. The CISSP Certification is administered by the International Information Systems Security Certification Consortium or (ISC)². The CISSP certification provides information security professionals with not only an objective measure of competence, but a globally recognized standard of achievement.

You Must Know!

Hours:
40 Academic Hours

Who should attend?

Experienced IT security-related practitioners, auditors, consultants, investigators or instructors, including network or security analysts and engineers, network administrators, information security specialists and risk management professionals, who wish to advance their current computer security careers

CISSP – certification Course

Course modules

Module 1 - 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

Module 2 - 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)

Module 3 - 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

Module 4 - Communication and Network Security

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

Module 5 - Identity and Access Management

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

Module 6 - 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

Module 7 - 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

Module 8 - Software Development Security

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

תל אביב

המרץ 2

CISSP – certification Course