MERCURY

Certified Information Systems Security Professional (CISSP)

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Certified Information Systems Security Professional (CISSP)

Introduction:

This Certified Information Systems Security Professional CISSP is a globally recognized certification in the field of information security, designed for IT security professionals to validate their knowledge and expertise in the ever-evolving cybersecurity landscape. The CISSP demonstrates an understanding of security concepts and practices, encompassing eight ISC² Common Body of Knowledge CBK domains. These domains include Security and Risk Management, Asset Security, Security Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

The CISSP certification is a professional's commitment to excellence in information security, enhancing their ability to develop, implement, and manage best-in-class cybersecurity. Professionals with skills and knowledge elevate their career prospects as organizations increasingly prioritize cybersecurity in their strategic objectives. Through examination, the CISSP empowers professionals to safeguard sensitive information and mitigate risks, positioning them as leaders in the security domain. Whether they are an aspiring cybersecurity expert or an experienced professional, pursuing the CISSP certification will advance their career and protect vital information assets.

This Certified Information Systems Security Professional CISSP training course is globally recognized in information security. The CISSP-certified information systems security professional has expertise in designing, implementing, and managing a cybersecurity program. It covers security architecture, risk management, software development security, and asset security, making it for those seeking to advance their cybersecurity careers.

The CISSP certification is achieved through rigorous study and training, often supported by a certified information systems security professional study guide, which provides structured preparation for the exam. By understanding CISSP meaning and undergoing CISSP training, professionals learn to become certified information systems security professionals and safeguard organizational data and infrastructure against evolving threats.

Targeted Groups:

- Information Security Managers.
- IT Security Professionals.
- Security Consultants.
- Network Architects.
- Systems Engineers.
- Security Auditors.
- Risk Assessment Professionals.
- Compliance Analysts.
- Chief Information Security Officers CISOs.
- Incident Response Teams.
- Security Analysts.
- Cloud Security Professionals.
- Data Protection Officers.
- Application Security Engineers.
- Business Continuity and Disaster Recovery Managers.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Course Objectives:

At the end of this Certified Information Systems Security Professional CISSP course, the participants will be able to:

- Equip participants with a comprehensive understanding of the eight domains of the ISC² CISSP Common Body of Knowledge CBK.
- Develop skills to identify and assess information security risks and implement appropriate mitigation strategies.
- Enable participants to design and implement effective security architectures and controls.
- Provide knowledge on managing identity and access within an organization's infrastructure.
- Teach effective techniques for conducting security assessments and penetration testing.
- Enhance understanding of incident response processes and recovery planning.
- Foster awareness of legal, regulatory, and compliance requirements in information security.
- Promote best practices for data protection and privacy management.
- Prepare participants for the CISSP certification exam through targeted study and practice resources.
- Cultivate leadership skills to manage and guide security teams and initiatives within an organization.

Targeted Competencies:

By the end of this Certified Information Systems Security Professional CISSP training, the participant's competencies will:

- Risk Management and Analysis.
- Security Architecture and Design.
- Identity and Access Management.
- Security Assessment and Testing.
- Security Operations Management.
- Incident Response and Recovery.
- Data Security and Privacy Protection.
- Network and Communications Security.
- Compliance and Regulatory Issues.
- Software Development Security.
- Business Continuity Planning.
- Threat and Vulnerability Management.
- Cloud Security Best Practices.
- Governance, Risk, and Compliance GRC.
- Security Awareness and Training.

Course Content:

Unit 1: Security and Risk Management:

- Understand the importance of security governance.
- Explore risk management concepts and frameworks.
- Learn how to develop and implement security policies and procedures.
- Identify legal and regulatory requirements for information security.
- Analyze risk assessment methodologies and tools.
- Discuss the role of security awareness training for employees.
- Examine business continuity and disaster recovery planning.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Unit 2: Asset Security:

- Define information assets and their classifications.
- Understand data ownership and responsibilities.
- Learn how to implement data retention and disposal policies.
- Explore methods for protecting data at rest, in transit, and in use.
- Identify security controls for various asset types.
- Discuss privacy protection measures and compliance requirements.
- Analyze the importance of maintaining asset inventories and valuations.

Unit 3: Security Architecture and Engineering:

- Explore security models and frameworks.
- Understand secure network architecture principles.
- Learn about security controls for physical and virtual environments.
- Discuss the role of cryptography in securing information.
- Analyze system and application security best practices.
- Understand the principles of secure coding and software development.
- Examine the impact of emerging technologies on security architecture.

Unit 4: Communication and Network Security:

- Understand network security concepts and protocols.
- Learn how to secure network architecture against threats.
- Explore techniques for secure remote access and communication.
- Discuss the implementation of firewalls, intrusion detection, and prevention systems.
- Analyze secure configurations for network devices.
- Understand the principles of wireless security.
- Learn about secure network monitoring and management practices.

Unit 5: Identity and Access Management:

- Define identity and access management IAM concepts.
- Understand authentication, authorization, and accounting AAA principles.
- Explore methods for managing user identities and access rights.
- Learn how to implement single sign-on SSO solutions.
- Discuss role-based access control RBAC and its benefits.
- Analyze access control models and frameworks.
- Understand the importance of identity federation and provisioning.