TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

# Certified Information system security professional Training CISSP

Often referred to as the 'gold standard', the Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security sector. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

Students will gain knowledge in information security that will increase their ability to successfully implement and manage security programs in any organization or government entity. The goal of this content is to provide students with the core knowledge necessary to be successful security professionals. This training course will help candidates review and refresh their information security knowledge in pursuit of the CISSP exam.

**Duration:**

5 days (40 hours)

**Exam:**

Length of exam: 4 hours

- **Target Audience:**
  - Chief Information Officer
  - Chief Information Security Officer
  - Chief Technology Officer
  - Compliance Manager/ Officer
  - Director of Security
  - Information Architect
  - Information Manager / Information Risk Manager or Consultant
  - IT Specialist/Director/Manager
  - Network/System Administrator

TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

- Security Administrator
- Security Architect / Security Analyst
- Security Consultant
- Security Manager
- Security Systems Engineer/ Security Engineer

**Learning Objectives:**

**Domain 1: Security and Risk Management**

- Justify an organizational code of ethics.
- Explain the ethical standards every professional security professional is expected to uphold.
- Specify the standards of behavior and performance expected of (ISC)2 members.
- Explain the security concepts of confidentiality, integrity, availability, authenticity, non-repudiation, privacy and safety.
- Relate security governance to organizational business strategies, goals, missions and objectives.
- Relate concepts and principles to due care and due diligence.
- Describe contractual, legal and industry standards, as well as regulatory requirements for information security.
- Explain how transborder data flow and import and export controls apply to data protection and privacy.
- Understand requirements for investigation types an organization may conduct in the case of a cyber incident.
- Review various privacy, cybersecurity and risk frameworks from an operational security perspective and as compliance requirements to their role in operational processes.
- Explain the overall organizational business continuity practice and the importance of the business impact analysis (BIA) to the planning process.
- Advocate for security considerations in personnel practices.
- Apply basic risk management theory to information security risks.

TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

- Demonstrate the readiness of the human component of organizational information security.

**Domain 2: Asset Security**

- Identify, classify, and categorize information assets.
- Explain the importance of treating information as an asset.
- Differentiate the IT asset management lifecycle from the data security lifecycle.
- Relate the data states of in use, in transit, and at rest to the data lifecycle.
- Relate the different roles that people and organizations have with respect to data.
- Describe the different security control types and categories.
- Explain the use of data security standards and baselines to meet organizational compliance requirements.

**Domain 3: Security Architecture and Engineering**

- Explain the significance of basic secure design principles.
- Compare and contrast the key security characteristics of security models.
- Explain the hardware foundations of security.
- Apply security principles to different information systems and their environments.
- Determine the best application of cryptographic approaches to solving organizational information security needs.
- Manage the use of certificates and digital signatures to meet organizational information security needs.
- Apply different cryptographic management solutions to meet organizational information security needs.
- Describe defenses against common cryptanalytic attacks.
- Apply the lessons of Crime Prevention through Environmental Design (CPTED) to information systems security design and operation.
- Identify information security implications of various physical facilities, systems and infrastructure.

TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

**Domain 4: Communication and Network Security**

- Describe the architectural characteristics, relevant technologies, protocols and security considerations of each of the layers in the Open Systems Interconnection (OSI) model.
- Explain the application of secure design practices in developing network infrastructure.
- Describe the evolution of methods to secure IP communications protocols.
- Explain the security implications of bound (cable and fiber) and unbound (wireless) network environments.
- Describe the evolution of, and security implications for, key network devices.
- Evaluate and contrast the security issues with voice communications in traditional and voice over internet protocol (VoIP) infrastructures.
- Describe and contrast the security considerations for key remote access technologies.
- Explain the security implications of software-defined networking (SDN) and network virtualization technologies.

**Domain 5: Identity and Access Management**

- Explain the identity lifecycle as it applies to human and nonhuman users.
- Compare and contrast access control models, mechanisms and concepts.
- Explain the role of authentication, authorization and accounting in achieving information security goals and objectives.
- Explain how IAM implementations must protect physical and logical assets.
- Describe the role of credentials and the identity store in IAM systems.

**Domain 6: Security Assessment and Testing**

- Describe the purpose, process and objectives of formal and informal security assessment and testing.
- Apply professional and organizational ethics to security assessment and testing.
- Explain internal, external and third-party assessment and testing.

TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

- Explain management and governance issues related to planning and conducting security assessments.
- Explain the role of assessment in data-driven security decision-making.

**Domain 7: Security Operations**

- Show how to efficiently and effectively gather and assess security data.
- Explain the security benefits of effective change management and change control.
- Develop incident response policies and plans.
- Link incident response to needs for security controls and their operational use.
- Relate security controls to improving and achieving required availability of information assets and systems.
- Understand the security and safety ramifications of various facilities, systems and infrastructure characteristics.

**Domain 8: Software Development Security**

- Recognize the many software elements that can put information systems security at risk.
- Identify and illustrate major causes of security weaknesses in source code.
- Illustrate major causes of security weaknesses in database and data warehouse systems.
- Explain the applicability of the Open Web Application Security Project (OWASP) framework to various web architectures.
- Contrast the ways that different software development methodologies, frameworks and guidelines contribute to information systems security.
- Explain the implementation of security controls for software development ecosystems.
- Choose an appropriate mix of security testing, assessment, controls and management methods for different systems and applications environments.