CISSP - Certified Information Systems Security Professional

Introduction

Certified Information Systems Security Professional CISSP® Certification is a globally recognized standard of achievement that confirms an individual's knowledge in the field of information security. CISSPs are information assurance professionals who define the architecture, design, management and/or controls that assure the security of business environments. It was the first certification in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024.

The CISSP exam is based on the following Ten domains:

1. Domain 1. Security and Risk Management
2. Domain 2. Asset Security
3. Domain 3. Security Architecture and Engineering
4. Domain 4. Communication and Network Security
5. Domain 5. Identity and Access Management (IAM)
6. Domain 6. Security Assessment and Testing
7. Domain 7. Security Operations
8. Domain 8. Software Development Security

Course Objectives

After completing this course, the student will be able to:

- Understand and apply fundamental concepts and methods related to the fields of information technology and security
- Align overall organizational operational goals with security functions and implementations
- Understand how to protect assets of the organization as they go through their lifecycle
- Understand the concepts, principles, structures and standards used to design, implement, monitor and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of confidentiality, integrity and availability
- Implement system security through the application of security design principles and application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures
- Understand the importance of cryptography and the security services it can provide in today's digital and information age
- Understand the impact of physical security elements on information system security and apply secure design principles to evaluate or recommend appropriate physical security protections

- Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function
- List the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1-7
- Identify standard terms for applying physical and logical access controls to environments related to their security practice
- Appraise various access control models to meet business security requirements
- Name primary methods for designing and validating test and audit strategies that support business requirements
- Enhance and optimize an organization's operational function and capacity by applying and utilizing appropriate security controls and countermeasures
- Recognize risks to an organization's operational endeavors and assess specific threats, vulnerabilities and controls
- Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it; identify which security control(s) are appropriate for the development environment; and assess the effectiveness of software security

Course Agenda

Domain 1: Security and Risk Management
Domain 2: Asset Security
Domain 3: Security Architecture and Engineering
Domain 4: Communication and Network Security
Domain 5: Identity and Access Management (IAM)
Domain 6: Security Assessment and Testing
Domain 7: Security Operations
Domain 8: Software Development Security