CISSP¬ Training and Certification Prep Course

Course: **00061**
Filter: **Beginner**
Duration: **4 days**
Category:: **Cyber Security**
Price: **2500,00 €**

About Course

The CISSP Training and Certification Prep Course is a comprehensive training course aimed at preparing individuals for the CISSP Certified Information Systems Security Professional exam. The course covers various aspects of information security, including security measures, data security, and system security. The curriculum also includes a focus on security architecture, application security, and cryptographic keys. Participants will learn about the ISC code of ethics and the CIA triad, as well as the trusted platform module (TPM) 2.0. Individuals who complete the course will gain a solid understanding of the skills and knowledge required to pass the CISSP exam, which is administered by Pearson VUE. To become CISSP certified, candidates must have a minimum of five years of work experience in the field of information security. The course also covers the latest developments in information security, including the requirements for operating systems and the impact of data breaches on sensitive information. Participants will learn about social engineering and the importance of a comprehensive information security program. The CISSP Training and Certification Prep Course provides the essential knowledge and skills required to become a CISSP-certified professional, with a focus on protecting the confidentiality, integrity, and availability of information. Passing the CISSP Certification Exam meets U.S. DoD Directive 8140/8570.01 Technical (IAT) Level-III, Information Assurance Security Architect/Engineer (IASAE) Level-I, Information Assurance Security Architect/Engineer (IASAE) Level-II, Management (IAM) Level-II, Management (IAM) Level-III requirements.

What you'll learn

- Manage security and risk.
- Practice securing assets.

- Design security framework.
- Secure communication and networks.
- Securely develop software.
- Learn from official (ISC)²® real-world instructors using (ISC)² course materials with a preferred official partner.
- Get practical insights into the 8 domains of the CISSP CBK (Common Body of Knowledge).
- Create a test study strategy by assessing strengths and weaknesses.
- Gain access to hundreds of exam prep questions.
- Receive a voucher for the CISSP certification exam included with the course tuition.
- Continue learning and face new challenges with after-course one-on-one instructor coaching.

Pre-requisites

- To succeed in this course and pass the exam, you should meet the specific requirements established by (ISC)².
- If you do not have the required experience, you should consider taking the Associate of (ISC)² exam first.

Curriculum

Module 1: Security and Risk Management

- In this module, you will learn how to:
- Understand, adhere to, and promote professional ethics
- Understand and apply security concepts
- Evaluate and apply security governance principles
- Determine compliance and other requirements
- Determine compliance and other requirements
- Understand legal and regulatory issues that pertain to information security in a holistic context

- Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply Supply Chain Risk Management (SCRM) concepts
- Establish and maintain a security awareness, education, and training program

Module 2: Asset Security

- In this module, you will learn how to:
- Identify and classify information and assets
- Establish information and asset handling requirements
- Provision resources securely
- Manage data lifecycle
- Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))
- Determine data security controls and compliance requirements

Module 3: Security Architecture and Engineering

- In this module, you will learn how to:
- Research, implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
- Select controls based upon systems security requirements
- Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
- Select and determine cryptographic solutions
- Understand methods of cryptanalytic attacks
- Apply security principles to site and facility design

- Design site and facility security controls

Module 4: Communication and Network Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Module 5: Identity and Access Management (IAM)

- In this module, you will learn how to:
- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

Module 6: Security Assessment and Testing

- In this module, you will learn how to:
- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate a report
- Conduct or facilitate security audits

Module 7: Security Operations

- In this module, you will learn how to:
- Understand and comply with investigations
- Conduct logging and monitoring activities
- Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)
- Apply foundational security operations concepts
- Apply resource protection
- Conduct incident management

- Operate and maintain detective and preventative measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Module 8: Software Development Security

- In this module, you will learn how to:
- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in software development ecosystems
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure code