Certified Information Systems Security Professional (CISSP) Training Course

CISSP is a globally recognized certification that validates advanced knowledge and skills in designing, implementing, and managing high-level cybersecurity programs.

SEC-301

Course Outcomes

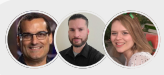
Professional, practical, & hands-on live instructor-led training

Advance your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career moving.

Start Today

Potential Career Tracks

- Information Security Manager
- Security Analyst
- IT Director/Manager
- Security Consultant
- Chief Information Security Officer
- Network Architect



Taught by Industry Veterans &
World Class Instructors

Introduction to Certified Information Systems Security Professional (CISSP)

Course Overview

Intellectual Point's Certified Information Systems Security Professional (CISSP) Training Course is meticulously crafted to equip security professionals with a comprehensive understanding of information security. This course covers the eight domains of the ISC2 CISSP Common Body of Knowledge, combining theoretical concepts with practical applications to ensure a holistic learning experience. Participants will gain the skills necessary to effectively design, implement, and manage a best-in-class cybersecurity program, reflecting real-world demands of the security landscape. Whether you are looking to advance your career or deepen your expertise in security management, this course will serve as a pivotal step in achieving those goals.

Throughout the training, you will delve into domains such as Security and Risk Management, Asset Security, and Security Engineering. You'll engage in interactive scenarios that help solidify your understanding of complex concepts, and apply these in practice labs tailored to real-world security challenges. By the end of the course, you will be well-prepared to tackle the CISSP certification exam and escalate your competence in the information security field.

Obtainable Skills

- Risk Management
- Asset Security
- Security Engineering
- Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security
- Incident Response

Course Insights

Audience Profile

The CISSP Training Course at Intellectual Point is designed for experienced IT professionals and cybersecurity specialists who aspire to validate and enhance their security management skills. This course is especially beneficial for IT managers, security consultants, and professionals with a minimum of five years of paid work experience in two or more of the CISSP domains. It is ideal for those interested in leadership roles in cybersecurity and looking to solidify their knowledge with a globally recognized credential. Additionally, security officers seeking to stay updated with current best practices will find tremendous value in this program.

Course Outcomes

By the end of this course, participants will:

1. Master the principles of information security risk management and governance.
2. Design and implement robust security architectures to safeguard organizational assets.
3. Develop and maintain an effective security operations framework.
4. Execute security assessments and tests to ensure compliance and protect infrastructures.
5. Prepare comprehensively for the CISSP certification, thereby advancing career and salary potential.

Module by Module Learning *Outline*

6 Modules

Module 1: Security and Risk Management

Learning Objectives:

- Understand the frameworks and principles of information security governance.
- Learn to identify, assess, and prioritize risks within an organization.

Topics Covered

Introduction to Security Governance:

- Concepts and principles of governance within cybersecurity.
- Establishing an effective security governance framework.

Risk Management Processes:

- Identification and assessment of risks.
- Strategies for mitigating and managing risk.

Module 2: Asset Security

Learning Objectives:

- Comprehend the classification and handling of organizational information and assets.
- Implement appropriate security and protective measures for asset management.

Topics Covered

Information and Asset Classification:

- Understanding asset valuation and sensitivity.
- Methods for classifying and safeguarding information.

Protecting and Securing Assets:

- Access control and monitoring of critical assets.
- Best practices for physical and logical asset protection.

Module 3: Security Engineering

Learning Objectives:

- Gain expertise in secure design principles and engineering processes.
- Learn to manage vulnerabilities and protective measures in systems.

Topics Covered

Security Models and Architecture:

- Principles of secure architecture in system design.
- Implementing security models to enforce policies.

Engineering Secure Systems:

- Addressing system vulnerabilities and threats.
- Incorporating security within the system development lifecycle (SDLC).

Module 4: Network Security

Learning Objectives:

- Develop skills to secure network infrastructures against threats.
- Explore technologies and protocols essential for network defense.

Topics Covered

Secure Network Design:

- Principles for designing and securing network architecture.
- Configuring network devices for optimal security.

Network Protocols and Security:

- Overview of key network protocols and their vulnerabilities.
- Implementing secure communication channels and measures.

Module 5: Identity and Access Management

Learning Objectives:

- Understand mechanisms and processes for effective identity and access control.
- Explore authentication and authorization techniques for robust security.

Topics Covered

Authentication Processes:

- Various methods and technologies for user authentication.
- Implementing multi-factor authentication (MFA) schemes.

Authorization and Access Control:

- Managing permissions and access rights.
- Employing role-based and least privilege access controls.

Module 6: Security Assessment and Testing

Learning Objectives:

- Conduct comprehensive security assessments to identify and mitigate vulnerabilities.
- Learn testing methodologies and tools for system evaluation.

Topics Covered

Security Testing Techniques:

- An overview of penetration testing and vulnerability assessments.
- Tools and frameworks for effective security testing.

Compliance and Audit Processes:

- Conducting audits to ensure regulatory compliance
- Reporting and remediation of findings from assessments.