CISSP: CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

Course Introduction:

The **Certified Information Systems Security Professional (CISSP)** is an advanced-level certification for IT pros serious about careers in information security. Offered by the International Information Systems Security Certification Consortium, known as **(ISC)2** (pronounced, "ISC squared"), this vendor-neutral credential is recognized worldwide for its standards of excellence.

CISSP credential holders are decision-makers who possess expert knowledge and technical skills necessary to develop, guide and manage security standards, policies and procedures within their organizations. The **CISSP** continues to be highly sought after by IT professionals and organizations. It is a regular fixture on most-wanted and must-have security certification surveys.

This course is the most comprehensive review of information security concepts and industry best practices, and focuses on the eight domains of the **CISSP CBK (Common Body of Knowledge)** that are covered in the **CISSP Exam**. You will gain knowledge in information security that will increase your ability to successfully implement and manage security programs in any organization or government entity.

What You'll Learn:

THIS COURSE PROVIDES IN-DEPTH COVERAGE OF THE EIGHT DOMAINS REQUIRED TO PASS THE CISSP EXAM:

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

Prerequisites:

You should have a minimum of five years of experience working in IT Infrastructure and Cybersecurity.

Who should attend?:

- Anyone whose position requires **CISSP** certification
- Individuals who want to advance within their current computer security careers or migrate to a related career

GLOBAL
IT TRAINING

Ready to Advance Your Career?
(919) 283-1653
sales@globalittraining.net

CISSP: CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

Course Outline:

1) Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity)

- Understand and Apply Concepts of Confidentiality, Integrity, and Availability
- Apply Security Governance Principles
- Compliance
- Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
- Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines
- Understand Business Continuity Requirements
- Contribute to Personnel Security Policies
- Understand and Apply Risk Management Concepts
- Understand and Apply Threat Modeling
- Integrate Security Risk Considerations into Acquisitions Strategy and Practice
- Establish and Manage Security Education, Training, and Awareness

2) Asset Security (Protecting Security of Assets)

- Classify Information and Supporting Assets
- Determine and Maintain Ownership
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Establish Handling Requirements

3) Security Engineering (Engineering and Management of Security)

- Implement and Manage an Engineering Life Cycle Using Security Design Principles
- Understand Fundamental Concepts of Security Models
- Select Controls and Countermeasures Based Upon Information Systems Security Standards
- Understand the Security Capabilities of Information Systems
- Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
- Assess and Mitigate Vulnerabilities in Web-based Systems
- Assess and Mitigate Vulnerabilities in Mobile Systems
- Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems
- Apply Cryptography
- Apply Secure Principles to Site and Facility Design
- Design and Implement Facility Security

4) Communications and Network Security (Designing and Protecting Network Security)

- Apply Secure Design Principles to Network Architecture
- Securing Network Components
- Design and Establish Secure Communication Channels
- Prevent or Mitigate Network Attacks

5) Identity and Access Management (Controlling Access and Managing Identity)

- Control Physical and Logical Access to Assets
- Manage Identification and Authentication of People and Devices
- Integrate Identity as a Service (IDaaS)
- Integrate Third-Party Identity Services
- Implement and Manage Authorization Mechanisms
- Prevent or Mitigate Access Control Attacks
- Manage the Identity and Access Provisioning Life Cycle

6) Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

- Design and Validate Assessment and Test Strategies
- Conduct Security Control Testing
- Collect Security Process Data
- Conduct or Facilitate Internal and Third-Party Audits

7) Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

- Understand and Support Investigations
- Understand Requirements for Investigation Types
- Conduct Logging and Monitoring Activities
- Secure the Provisioning of Resources through Configuration Management
- Understand and Apply Foundational Security Operations Concepts
- Employ Resource Protection Techniques
- Conduct Incident Response
- Operate and Maintain Preventative Measures
- Implement and Support Patch and Vulnerability Management
- Participate in and Understand Change Management Processes
- Implement Recovery Strategies
- Implement Disaster Recovery Processes
- Test Disaster Recovery Plan
- Participate in Business Continuity Planning
- Implement and Manage Physical Security
- Participate in Personnel Safety

8) Software Development Security (Understanding, Applying, and Enforcing Software Security)

- Understand and Apply Security in the Software Development Life Cycle
- Enforce Security Controls in the Development Environment
- Assess the Effectiveness of Software Security
- Assess Software Acquisition Security

GLOBAL
IT TRAINING

Ready to Advance Your Career?
(919) 283-1653
sales@globalittraining.net