Clemson University - Center for Corporate Learning
1 North Main Street, 7th Floor,
Greenville, SC 29601
http://www.clemson.edu/online/
Contact: Juanita Durham | 864.656.3984 | jdrhm@clemson.edu

Certified Information Security Systems Professional (CISSP)

Format:	Self-Pace Online / eLearning
Program Duration:	6 Months
Course Contact Hours:	375

The Certified Information Security Systems Professional (CISSP) Profession

CISSP certified individuals know how to get an organization to meet the information system security challenge, now and moving forward. Certified Information Systems Security Professional (CISSP) is an information security certification developed by the International Information Systems Security Certification Consortium, also known as (ISC)². The CISSP designation is a globally recognized, vendor-neutral standard for attesting to an IT security professional's technical skills and experience in implementing and managing a security program. The CISSP is a certification sought by IT professionals with job titles such as security auditor, security systems engineer, security architect and chief information security officer, among others.

The Certified Information Security Systems Professional (CISSP) Program

The Certified Information Systems Security Professional material introduces participants to all eight domains of advanced security knowledge covered on the CISSP exam. Participants learn how to model threats, assess risks, plan business continuity, protect assets, and engineer strong security into complex systems. Participants also learn how to protect networks, communications, access, and identities; assess and test security, and manage security operations. Once complete, participants will have core skills for designing, implementing, and managing IT security for entire organizations.

Education and National Certifications

- Students should have or be pursuing a high school diploma or GED.
- National Certification:
  - **Certified Information Systems Security Professional (CISSP) certification from (ISC)²**
  - **IMPORTANT: In addition to this training program, earning certification requires the following:**
    - **5 years of security work experience:** You must be able to show proof of five paid full-time years of work experience in at least two of the eight CISSP CBK (Common Body of Knowledge) domains, which are Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

- **Get endorsed to become a CISSP:** Once you complete the CISSP exam, you'll have to subscribe to the (ISC)^2 Code of Ethics and complete an endorsement form to become a CISSP. The endorsement form must be signed by another (ISC)^2 certified professional who verifies your professional work experience. You must submit the completed form within nine months of passing your exam to become fully certified, because passing the exam doesn't automatically grant you certification status.

Program Objectives

At the conclusion of this program, students will be able to:

- Summarize DNS concepts and its components, and increasingly converged networks
- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security
- Becoming a CISSP

Certified Information Security Systems Professional (CISSP) Detailed Student Objectives

DOMAIN 1: SECURITY AND RISK MANAGEMENT

SECURITY AND RISK MANAGEMENT PART 1

- Examining Information Security Fundamentals
- Applying Security Governance Concepts – Part 1
- Applying Security Ggoernance Concepts – Part 2
- Designing and implementing governance documents
- Understadnign legal systems and related laws – Part 1
- Understanding legal systems and related laws – Part 2
- Implementing Personnel Security
- Implementing Third-Party Security

SECURITY AND RISK MANAGEMENT PART 2

- Understanding and Applying Threat Modeling
- Understanding & Implementing Risk Management Concepts
- Exploring Risk Assessment Methodologies
- Conducting a Quantitative Risk Assessment
- Conducting a Qualitative Risk Assessment
- Selecting Controls and Countermeasures
- Managing Supply Chain Risk
- Implementing Business Continuity Risk Management

DOMAIN 2: ASSET SECURITY

ASSET SECURITY

- Classifying Assets
- Managing Assets
- Protecting Data Privacy
- Ensuring Appropriate Retention and Destruction
- Determining Data Security Controls

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

SECURITY ENGINEERING PART 1

- Implementing Secure Design Principles
- Understanding Security Models
- Selecting Controls Based on Systems Security Evaluation Models
- Recognizing Information Systems Security Capabilities
- Assessing and Mitigating Security Architecture Vulnerabilitiies
- Assessing and Mitigating Cloud Vulnerabilities
- Assessing and Mitigating Web Vulnrabilties
- Assessing and Mitigating Mobile and Remote Computing Vulnerabilities

SECURITY ENGINEERING PART 2

- Introducing Cryptography
- Applying Cryptography – Encryption Part 1
- Applying Cryptography – Encryption Part 2
- Applying Cryptography – Public Key Infrastructure
- Applying Cryptography – Hashing and Digital Signature
- Applying Cryptography – Crytography Protocols
- Applying Cryptography – Crypto Attacks
- Applying Secure Principles to Site and Facility Design
- Securing Information Processing Facilities and Equipment

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

COMMUNICATION AND NETWORK SECURITY

- Reviewing OSI and TCP/IP Models
- Understanding IP Convergence and Extensibility
- Securing Wireless Networks
- Using Cryptography to Maintain Communication Security
- Securing Network Access
- Securing Data Transmissions
- Securing Multimedia Collaboration
- Securing Virtual Private Networks
- Securing Endpoints
- Preventing and Migrating Network Attacks

DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT (IAM)

IDENTITY AND ACCESS MANAGEMENT

- Understanding Access Control Fundamentas
- Examining Identification Schemes
- Understanding Authentication Options

- Understanding Authentication Systems
- Implementing Access and Authorization Criteria
- Implementing Access Control Models
- Implementing Access Control Techniques and Technologies
- Identify and Access Provisioning

DOMAIN 6: SECURITY ASSESSMENT AND TESTING

SECURITY ASSESSMENT AND TESTING

- Testing and Examination (T&E) Overview
- Security Assessment Planning
- Conducting Security Examinations
- Conducting Security Testing – Target Identification
- Conducting Security Testing – Password Cracking
- Conducting Security Testing – Penetration Testing
- Understanding Log Analysis
- Implementing Information Security Continuous Monitoring (ISCM)
- Understanding Third-Party Audits and Examination

DOMAIN 7: SECURITY OPERATIONS

SECURITY OPERATIONS – PART 1

- Managing Privileged Accounts
- Operating and Maintaining Firewalls and IDS/IPS
- Conducting Logging and Monitoring Activities
- Implementing and Supporting Vulnerability and Patch Management
- Implementing and Supporting Malware & Media Management
- Participating in the Configuration Management Process

SECURITY OPERATIONS – PART 2

- Managing System Resilience and Fault Tolerance
- Implementing Disaster recovery Processes
- Managing DR Plan Maintenance
- Understanding and Supporting Investigations
- Understanding Digital Forensics
- Supporting Incident Management
- Securing People and Places

DOMAIN 8: SOFTWARE DEVELOPMENT SECURITY

SOFTWARE DEVELOPMENT SECURITY

- Managing the Software Development Lifecycle
- Understanding Software Development Approaches, Models and Tools
- Understanding Source Code Security Issues
- Managing Database Security
- Assessing the Security Impact of Acquired Software

DOMAIN 9: BECOMING A CISSP

PREPARING FOR THE EXAM

- Security and Risk Managementt Domain: Review and Study Roadmap
- Asset Security Domain: Review and Study Roadmap
- Security Engineering Domain: Review and Study Roadmap
- Communications and Network Security Domain: Review and Study Roadmap
- Identify and Access Domain: Review and Study Roadmap
- Secuity Assessment and Testing Domain: Review and Study Roadmap
- Security Operations Domain: Review and Study Roadmap
- Security Development Security Domain: Review and Study Roadmap
- Taking the CISSP Examination