Certified Information Systems Security Professional

CISSP

Course Syllabus

24 Hours

Course Description

The CISSP certification is the ideal credential for those with proven, deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks. Backed by (ISC)², the globally recognized, nonprofit organization dedicated to advancing the information security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement. This course covers the objectives for the certification exam:

- **Certified Information Systems Security Professional (CISSP)**

Learning Objectives

Upon completion of the course, students will understand:

- Establishing security governance principles and how best to establish and implement comprehensive security guidelines across an organization
- Best practices for personnel security, risk management concepts, and risk analysis techniques
- Function of threat modeling, countermeasure selection, and implementing risk controls
- Basis for risk monitoring and reporting best practices
- Privacy protection considerations, including data remanence and collection limitations
- Best practices for media, hardware and personnel retention, and techniques for determining most appropriate data security controls like scoping, tailoring and cryptography
- Analysis of security threats, both natural and man-made, and techniques for preventing loss from these threats
- Considerations in site and facility design, restricted work area security, and best practices for crime prevention through secure design of physical environment
- Components of network systems, how to implement secure systems, and how to mitigate common attacks
- Techniques for performing general security operations activities such as security investigations, including best practices and requirements for types of investigations that security professionals typically take part in
- Best practices for assessing software security effectiveness, such as using change logs and audits, software security risk analysis, and software security acceptance testing
- Organizational safety measures such as business continuity planning, managing physical security of premises, and addressing personnel safety concerns like employee monitoring and privacy policies
- Development and implementation of recovery strategies, including specific strategies for backup storage, recovery sites, multiple processing sites, and system resilience and fault tolerance requirements
- Techniques for using logging and monitoring activities for security purposes, establishing secure resource provisioning, and applying general security concepts such as least privilege to all security operations activities
- Best practices for assessing software security effectiveness, such as using change logs and audits, software security risk analysis, and software security acceptance testing

Course Format

CISSP is a self-paced, online course delivered through the learning management system Skillsoft. The site to access the coursework is su.skillport.com. Login credentials will be provided to you on the cohort launch date. If you do not receive them by the launch date, please check your Spam/Junk folder of your email and/or contact your advisor or O2O program coordinator. Once you have logged into your account, you can locate the coursework by selecting "View My Learning Plan."

Coursework is delivered through videos, tutorials, and tests. No textbooks are required for the course; however, students are encouraged to utilize additional resources to assist with certification preparation. Resource Guides with lists of supplemental study materials for each certification are available at http://libguide.get-vet.syr.edu/curriculum/.

Course Completion Requirements

CISSP coursework is due within 90 days from the assignment date. You must complete all 12 modules listed within Topic 1. Successful completion of a module is marked after you review the lesson videos and score 80% or higher on the end of module tests.

At the beginning of a module, you will be asked to take a pre-test. Scoring 80% or higher on the pre-test signifies competence in the information that will be covered; you will therefore be waived from completing the module. A non-credit certificate of completion will be awarded for successful completion of the coursework.

Industry Certification Requirements

In order for the program to fund your CISSP certification exam you will need to meet the CISSP practice exam requirements. Your advisor or O2O program coordinator will provide you with access to the practice exam as well as completion instructions once you have finished the coursework.

Support

- For technical support, please contact Skillsoft Support at support.skillsoft.com
- For course content support, please utilize Skillsoft's "Ask My Mentor" tool, located in the left-hand Menu within the module course player
- For program support or questions, please contact your advisor or O2O program coordinator

Course Outline

Topic 1: Advanced Security for CISSP Certification

1.1 CISSP: Security Principles, Governance, and Guidelines

1.2 CISSP: Risk Management

1.3 CISSP: Asset Security

1.4 CISSP: Security Engineering Part I

1.5 CISSP: Security Engineering Part II

1.6 CISSP: Communication & Network Security Design

1.7 CISSP: Identity and Access Management

1.8 CISSP: Security Assessment and Testing

1.9 CISSP: Security Operations Part I

1.10 CISSP: Security Operations Part II

1.11 CISSP: Security Operations Part III

1.12 CISSP: Software Development Security