

CISSP CERTIFICATION TRAINING

BE ON TOP OF YOUR CYBER SECURITY GAME



PROGRAM OVERVIEW

The Purdue official (ISC)² CISSP common body of knowledge workshop and examination make up an intensive program that covers a comprehensive collection of information security best practices. The eight security domains that will be covered are security and risk management; asset security; security architecture and engineering; communication and network security; identity and access management; security assessment and testing; security operations; and software development security.

HOW IT WORKS

- » Course Length: 1 week bootcamp
- » Schedule: M-F 8:00 a.m. - 5:00 p.m. (EST)
- » Format: 100% online, instructor-led live sessions

FEATURES

- » Live instructor-led training
- » Access to a lab platform that allows hands-on practice
- » Access to CertMaster Practice, a set of practice tests and real-time feedback that helps you train for the exam
- » Access to the electronic textbook
- » An exam voucher for up to one year

* Candidates must have a minimum of five years of cumulative paid work experience in two or more of the eight domains of the CISSP CBK.

WHO NEEDS THIS COURSE

Chief Information Officers
IT Director/Managers
Network Architects
Security Analysts
Security Architects
Security Consultants
Security Managers

WHY A CISSP CREDENTIAL?

On average, (ISC)² members report earning 35% more than non-members.

This certificate is vendor-neutral, so skills obtained can be applied to different technologies and methodologies.

Meets U.S. Department of Defense Directive 8570.1.

The first information security credential to meet the strict conditions of ISO/IEC Standard 17024.

The average CISSP salary, stated by (ISC)², is US \$131,030.

COURSE AGENDA

- › Domain 1: Security and Risk Management
- › Domain 2: Asset Security
- › Domain 3: Security Architecture and Engineering
- › Domain 4: Communication and Network Security
- › Domain 5: Identity and Access Management (IAM)
- › Domain 6: Security Assessment and Testing
- › Domain 7: Security Operations
- › Domain 8: Software Development Security

DAY 1: RISK MANAGEMENT

- › Security Governance
- › Evaluation of Compliance Requirements
- › Threat Modeling
- › Policy, Standards, Procedures, and Guidance
- › Business Continuity Requirements
- › Risk Management Concepts in the Supply Chain

DAY 2: ASSET SECURITY

- › Protecting Privacy
- › Data Security Controls (Data Loss Prevention)
- › Secure Design Principles
- › Security Capabilities of Information System Cryptography

DAY 3: OSI MODEL AND TCP MODEL

- › Network Security
- › Identity and Access Management
- › Multi-factor Authentication Biometrics

DAY 4: SECURITY CONTROL TESTING

- › Analyze Vulnerability Scan Reports and Generating Report
- › Security Audits
- › Digital Forensics
- › Configuration Management
- › Incident Management
- › Disaster Recovery Physical Security

DAY 5: PERSONNEL SECURITY

- › Log Management
- › Software Development Life Cycle
- › Software Security (Auditing, Logging, Risk Analysis, and Mitigation)
- › Secure Coding Standards and Guidelines
- › Security Controls in Development Environments

CISSP CERTIFICATION

JOB OUTLOOK



CYBER JOBS OPEN IN THE
U.S. IN 2021

ACCORDING TO CYBERCRIME MAGAZINE

PAY SCALE

SALARY AVERAGE

\$131,030

CISSP.COM

JOB TITLES

CHIEF INFORMATION SECURITY OFFICER
CHIEF INFORMATION OFFICER
SECURITY SYSTEMS ENGINEER
SECURITY ANALYST
SECURITY MANAGER
SECURITY AUDITOR
SECURITY CONSULTANT
NETWORK ARCHITECT
IT DIRECTOR OR MANAGER
DIRECTOR OF SECURITY

CISSP.COM

**140,000
MEMBERS**

JOIN THE WORLDS LARGEST ASSOCIATION
OF CYBERSECURITY PROFESSIONS

CISSP.COM