Certified Information Systems Security Professional (CISSP)
Training Program Overview & Outline

Training Overview

This five-day day training program focuses on the eight domains in the ISC2 CCSP Common Body of Knowledge, including:

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

Practical “how to” guidance and sample questions are provided to enhance the students’ exam readiness.

Note: BAI provides training and test preparation. The exam itself is administered by ISC2.

Introduction

Backed by (ISC)2, CISSP credentialing is the “gold standard” in cybersecurity. This cybersecurity certification is an elite way to demonstrate your knowledge, advance your career, and become a member of a community of cybersecurity leaders.

Prerequisites

Candidates must have five years of cumulative paid full-time information technology work experience, of which two or more years must be in two or more of the eight domains of the (ISC)2 Common Body of Knowledge (CBK). An alternative option is to take and pass the CISSP exam to earn an Associate of (ISC)2 designation.

* Students can satisfy one year of required experience with a four-year college degree or an approved credentials from the CISSP Prerequisite pathway.

Who Should Become a CISSP

- Security Consultant
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- IT Director/Manager
- Director of Security
- Network Architect
- Security Systems Engineer
- Chief Information Security Officer

CISSP® Certified Information Systems Security Professional

BAI Information Security Consulting & Training
Risk Management Framework (RMF) Resource Center
1-800-RMF-1903 (763-1903)
www.rmf.org

Certified Information Systems Security Professional (CISSP)

Training Program Overview & Outline

Domain 1: Security and Risk Management

- Confidentiality, integrity, and availability concepts
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethic
- Security policies, standards, procedures and guidelines

Domain 2 Asset Security

- Information and asset classification
- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)

Domain 3 Security Engineering

- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

Domain 4 Communication & Network Security

- Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

Domain 5 Identity and Access Management

- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service (e.g. cloud identity)
- Third-party identity services (e.g. on-premise)
- Access control attacks
- Identity and access provisioning lifecycle (e.g. provisioning review)

Domain 6 Security Assessment and Testing

- Assessment and test strategies
- Security process data (e.g. management and operational controls) •
- Security control testing
- Test outputs (e.g. automated, manual) •
- Security architectures vulnerabilities

Domain 7 Security Operations

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Domain 8 Software Development Security

- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact