Hands-On

CISSP Certification Prep

Course Description

The CISSP training is an advanced course designed to meet the high demands of the information security industry by preparing students for the Certified Information Systems Security Professional (CISSP) exam.

Led by an Authorized Instructor, this training course provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of the CISSP CBK

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communications and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

The CISSP Helps You

-Validate your proven competence gained through years of experience in information security

-Demonstrate your technical knowledge, skills, and abilities to effectively develop a holistic security program set against globally accepted standards

-Differentiate yourself from other candidates for desirable job openings in the fast-growing information security market

-Affirm your commitment to the field and ongoing relevancy through continuing professional education and understanding of the most current best practices

-Gain access to valuable career resources, such as networking and ideas exchange with peers

The CISSP Helps Employers

-Protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure business environment

-Ensure professionals stay current on emerging threats, technologies, regulations, standards, and practices through the continuing professional education requirements

-Increase confidence that candidates are qualified and committed to information security

-Ensure employees use a universal language, circumventing ambiguity with industry-accepted terms and practices

-Increase organizations' credibility when working with clients and vendors

Students Will Learn

- **Understand and apply the concepts of risk assessment, risk analysis, data classification, and security awareness and Implement risk management and the principles used to support it (Risk avoidance, Risk acceptance, Risk mitigation, Risk transference)**
- **Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and address the frameworks and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets, as well as to assess the effectiveness of that protection and establish the foundation of a comprehensive and proactive security program to ensure the protection of an organization's information assets**
- **Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and examine the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality, and authenticity.**
- **Understand the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media and identify risks that can be quantitatively and qualitatively measured to support the building of business cases to drive proactive security in the enterprise.**
- **Offer greater visibility into determining who or what may have altered data or system information, potentially affecting the integrity of those asset and match an entity, such as a person or a computer system, with the actions that entity takes against valuable assets, allowing organizations to have a better understanding of the state of their security posture.**
- **Plan for technology development, including risk, and evaluate the system design against mission requirements, and identify where competitive prototyping and other evaluation techniques fit in the process.**
- **Protect and control information processing assets in centralized and distributed environments and execute the daily tasks required to keep security services operating reliably and efficiently.**
- **Understand the Software Development Life Cycle (SDLC) and how to apply security to it, and identify which security control(s) are appropriate for the development environment, and assess the effectiveness of software security.**
- **And Much More...**

Target Audience

This training course is intended for professionals who have at least 5 years of recent full-time professional work experience in 2 or more of the 8 domains of the CISSP CBK and are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current information security careers. The training seminar is ideal for those working in positions such as, but not limited to

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

Prerequisites

Candidates must have a minimum of five (5) years of cumulative paid full-time professional security work experience in two or more of the 8 domains of the CISSP CBK.

Candidates may receive a one year experience waiver with a four-year college degree, or regional equivalent OR additional credential from the approved list, thus requiring four (4) years of direct full-time professional security work experience in two or more of the ten domains of the CISSP CBK.

Candidates who have not completed the 5 years of experience to take the CISSP, can take an Associate CISSP exam. This will give them a credential showing their knowledge until they are able to meet the experience requirements for the CISSP.

Course Outline

Security and Risk Management

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

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)

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

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

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)

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

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

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

Delivery Method

Instructor-Led with Labs and exercises throughout (Virtual and On-Site Delivery Available).

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

5 Days