Hands-On

CISSP Training Boot Camp

Course Description

BTS now is delivering a highly-rated 5 or 10 Day CISSP Boot Camp to the Information Security community. This course will prepare you to pass the premier security certification, the Certified Information Systems Security Professional (CISSP).

Information Technology Professionals earning the CISSP have definitive knowledge of the ten Common Body of Knowledge (CBK) Domains, and have skills to provide leadership in security related tasks for enterprise wide information security programs.

If you are in the IT Profession an IT professional, take our CISSP certification training course to get the knowledge and skills needed to pass the CISSP exam.

The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 170242003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

It is also a Level II DoD regulation 8570 requirement for Military, Government and Defense Contractors working in security related areas of IT.

Note This course can be delivered in a 5-day, 7-Day and a 10 Day format depending on scope and background of the attendees.

Students Will Learn

- **Access Control**
- **Application Security**
- **Business Continuity and Disaster Recovery Planning**
- **Cryptography**
- **Information Security and Risk Management**
- **Legal, Regulations, Compliance and Investigations**
- **Operations Security**
- **Physical (Environmental) Security**
- **Security Architecture and Design**
- **Telecommunications and Network Security**
- **And More...**

Target Audience

If you are in the IT Profession an IT professional, take our CISSP certification training course to get the knowledge and skills needed to pass the CISSP exam.

Prerequisites

Attendees must pass their Security+ exam, if they take the 5-day delivery of this CISSP course. Professional work experience in one or more of the ten test domains of the information systems security would be highly recommended.

Course Outline

- **Access Control** - A collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

- **Telecommunications and Network Security** - Network structures; transmission methods; transport formats; security measures used to provide availability, integrity, and confidentiality; and authentication for transmissions over private and public communications networks and media.

- **Information Security Governance and Risk Management** - The identification of an organizations information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. Management tools such as data classification and risk assessment/analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented.

- **Software Development Security** - Addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.

- **Cryptography** - The principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

- **Security Architecture and Design** - Contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality.

- **Operations Security** - Used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the

pertinent information to the appropriate individual, group, or process.

- **Business Continuity and Disaster Recovery Planning** - For the preservation and recovery of business operations in the event of outages.

- **Legal, Regulations, Investigations and Compliance** - Computer crime laws and regulations and the measures and technologies used to investigate computer crime incidents.

- **Physical (Environmental) Security** - Provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.

Delivery Method

Instructor-Led with numerous Hands-On labs and exercises.

Equipment Requirements

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

Hands-On Instructor-Led with numerous exercises.

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