

## Course Description

This course meets the NEW DoD Directive 8140 requirements.

Will Department of Defense (DoD) Directive 8140 replace DoDD 8570? Yes.

When will DoD 8140 take effect? It is already in effect.

Why Change from 8570 to 8140?

DoD 8140 is designed to be more flexible and inclusive than DoD 8570. DoD 8140 includes initiatives such as NIST NICE (National Initiative for Cybersecurity Education), which identifies critical KSAs (Knowledge, Skills, and Abilities) and places cybersecurity positions into 7 categories (1. Security Provision, 2. Operate & Maintain, 3. Protect & Defend, 4. Analyze, 5. Operate & Collect, 6. Oversight & Development, and 7. Investigate) consisting of 31 specialty areas.

CompTIA's Security+ (DOD8410) is the premier vendor-neutral security certification and demonstrates your knowledge of security concepts, tools, and procedures. It confirms your ability to react to security incidents, and it validates your skill in anticipating security risks and guarding against them.

In this course, you will learn to proactively implement sound security protocols to mitigate security risks, quickly respond to security issues, and retroactively identify where security breaches may have occurred. You will also learn to design a network, on-site or in the cloud, with security in mind.

Our Security+ Prep Course prepares you for the Security+ certification exam based on the New 8410, which is included in the approved list of certifications.

BTS works with clients to deliver appropriate material to become CompTIA Security+ certified.

## Students Will Learn

- **Mitigating threats**
- **Cryptography**
- **Authentication**
- **User and role-based security**
- **Peripheral security**
- **Public key infrastructure**
- **Application and messaging security**
- **Ports and protocols**
- **Network security**

- **Wireless security**
- **Remote access security**
- **Auditing, logging, and monitoring**
- **Vulnerability testing and monitoring**
- **Organizational security**
- **Business continuity**
- **CompTIA Security+ objectives map**
- **CompTIA Security+ acronyms**

## Target Audience

Anyone interested in Security+ certification (SY0-301).

## Prerequisites

CompTIA A+ and Network+ certifications, or equivalent knowledge. Experience in networking, including experience configuring and managing TCP/IP is beneficial.

## Course Outline

### 1. Mitigating Threats

- System maintenance
- Application security
- Physical security
- Malware
- Social engineering

### 2. Cryptography

- Symmetric cryptography
- Public key cryptography

### 3. Authentication

- Authentication factors and requirements
- Authentication systems
- Authentication system vulnerabilities

### 4. User- and Role-Based Security

- Baseline security policies
- Resource access

### 5. Peripheral Security

- File and disk encryption

- Peripheral and component security
  - Mobile device security
6. Public Key Infrastructure
    - Public key cryptography
    - Implementing public key infrastructure (PKI)
    - Web server security with PKI
  7. Application and Messaging Security
    - Application security
    - E-mail security
    - Social networking and messaging
  8. Ports and Protocols
    - TCP/IP basics
    - Protocol-based attacks
  9. Network Security
    - Network devices
    - Secure network topologies
    - Secure networking
    - Virtualization and cloud computing
  10. Wireless Security
    - Wireless network security
    - Mobile device security
  11. Remote Access Security
    - Remote access
    - Virtual private networks
  12. Vulnerability Testing
    - Risk and vulnerability assessment
    - Auditing and logging
    - Intrusion detection and prevention systems
    - Incident response
  13. Organizational Security
    - Organizational policies
    - Education and training
    - Disposal and destruction
  14. Business Continuity
    - Redundancy planning
    - Disaster recovery
    - Environmental controls

## Delivery Method

Instructor led with numerous Hands-On labs and exercises.

## 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