# ISTQB - Security Test Engineer Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

What Can You Achieve with This Training?

- Develop an understanding of the **testing approaches and techniques** used to evaluate the security of software and IT-based systems.
- Strengthen your ability to perform structured security testing through **penetration testing, vulnerability scanning, and risk-based testing**.
- Use **threat modeling, security risk analysis, and test design** to align testing activities with organisational security risks.
- Select suitable **security testing tools** and evaluate the results produced during testing.
- Contribute to **security findings reporting, stakeholder communication, and vulnerability management**.
- Learn how to integrate security testing into the software development lifecycle using **OWASP, ISO 29119, and information security management** practices.

The **ISTQB – Security Test Engineer Training** is a **three-day technical course** intended for professionals involved in evaluating the security of IT-based systems.

The programme focuses on the **practical execution of security testing activities**, including the selection of appropriate tools, interpretation of results, and communication of security findings. Participants explore how security testing can be performed in different development environments and how its outcomes contribute to broader organisational risk management processes.

The course introduces **security paradigms, security testing techniques, test processes, standards, and recommended practices**. It also examines the influence of organisational structures, security policies, regulatory requirements, and attack scenarios on testing activities.

Further modules address the role of security testing throughout the **software development lifecycle (SDLC)**, including operational and maintenance activities. Participants learn how security testing relates to an **Information Security Management System (ISMS)**, how acceptance criteria are established, and how testing processes can be improved.

The training also covers **security test reporting, vulnerability analysis, vulnerability management, and the use of security testing tools**.

Designed for professionals seeking to improve their security testing capabilities, the course supports more effective participation in **secure software delivery**.

## Prerequisites

# ISTQB - Security Test Engineer Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Candidates must hold an **ISTQB Foundation Level certification** before taking the associated examination.

**Certification Prerequisite**

An **ISTQB Foundation Level certification** is required before taking the associated **ISTQB Security Test Engineer** examination.

## Who Should Attend

This course is intended for professionals involved in **security testing of software and IT systems**, as well as those seeking to develop specialist skills in this area.

It is particularly relevant to:

- **Software Testers**
- **Security Test Engineers**
- **Quality Assurance (QA) Professionals**
- **Software and Application Security Specialists**
- **Test Leads and Test Managers**
- **IT Professionals involved in security testing activities**

# ISTQB - Security Test Engineer Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## What You Will Learn

By the end of this course, participants will be able to:

- Explain the fundamental **principles, concepts, and terminology of ISTQB security testing**.
- Evaluate and apply security testing techniques, including **penetration testing and vulnerability scanning**.
- Analyse security risks using **threat modeling and risk-based testing** approaches.
- Develop **security test plans** aligned with organisational risk management and compliance requirements.
- Select and use appropriate **security testing tools** within different software delivery environments.
- Interpret **security test results**, prepare reports, and communicate findings effectively to stakeholders.
- Apply relevant standards and practices, including **OWASP and ISO 29119**, to security testing activities.
- Integrate security testing throughout the **software development lifecycle (SDLC)**.
- Relate **Zero Trust, security audits, and asset security** concepts to security testing practices.
- Analyse **attack scenarios** to support security test design.
- Explain how security test results contribute to risk management within an **Information Security Management System (ISMS)**.
- Support **vulnerability analysis and vulnerability management** activities.
- Identify opportunities for **continuous improvement of security testing processes** within an organisation.

## Outline

### 1. Security Paradigms

- Examining **asset security levels** and their role in security assessment
- Understanding the purpose of **security audits** and their relationship to security testing
- Introducing fundamental **Zero Trust** concepts
- Evaluating **open-source software** from a security perspective

### 2. Security Test Techniques

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Reviewing different **security test types** and their applications
- Applying appropriate **security testing techniques** in relevant scenarios
- Designing **security tests** and selecting suitable testing approaches

### 3. Security Test Process

- Understanding the key activities within the **security testing process**
- Designing **security test cases and test scenarios** based on testing requirements
- Evaluating important considerations during **test execution**

### 4. Standards and Best Practices

- Exploring **security testing standards** and their areas of application
- Applying recognised **security testing best practices**
- Using **standards** to guide the planning and execution of testing activities

### 5. Organisational Context

- Examining how **organisational structures** influence security testing
- Reviewing **security policies and regulatory requirements**
- Analysing **attack scenarios** in the context of security testing

### 6. Software Development Lifecycle

- Comparing different **software development lifecycle models**
- Understanding how **security testing is performed during operations**
- Addressing security testing within **software maintenance activities**

### 7. Information Security Management

- Exploring **Information Security Management Systems (ISMS)** and their relationship to security testing
- Defining **acceptance criteria** for security testing activities
- Identifying approaches to **improving security testing processes**

### 8. Reporting and Vulnerabilities

- Preparing and communicating **security test reports**
- Performing **vulnerability analysis**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Understanding **vulnerability management** processes

### 9. Security Test Tools

- Identifying major **security testing tool categories** and their purposes
- Selecting and applying **security testing tools** according to testing needs