SECURITY TESTER

Security testing is based on the security aspect of functional specifications but also seeks to verify and validate security risks, security procedures and policies, attacker behavior and known security vulnerabilities.

Security test objectives are based on security risks. These risks are identified through performing a security risk assessment and the syllabus will show how to perform a security risk assessment.

Security testing assesses a system's vulnerability to threats by attempting to compromise the system's security policy.

Like software testing in general, security testing is also a lifecycle activity. Failure to implement and test security measures throughout a project can lead to severe security defects which never get fully resolved. The security test process that is defined within this syllabus must be aligned with your development process so that appropriate test activities are performed when needed.

The syllabus will also show you the Role of Security Testing in a Software Development Lifecycle. In one chapter you will learn the most important security testing mechanism (like intrusion detection, data obfuscation, etc.).

You will also learn to understand the attackers and the impact of human behavior on security risks.

The last three chapters show you how to measure and report security test results, what tools you could use and which standards and trends are available.

THE BASIS OF SECURITY TESTING	105 MIN.
SECURITY TEST PURPOSES, GOALS AND STRATEGIES	130 MIN.
SECURITY TESTING PROCESSES	140 MIN.
SECURITY TESTING THROUGHOUT THE APPLICATION LIFECYCLE	225 MIN.
TESTING SECURITY MECHANISMS	240 MIN.
HUMAN FACTORS IN SECURITY TESTING	105 MIN.
SECURITY TEST EVALUATION AND REPORTING	70 MIN.
SECURITY TESTING TOOLS	55 MIN.
STANDARDS AND INDUSTRY TRENDS	40 MIN.
TOTAL	1110 MIN.

STB
Swiss Testing Board

info@swiss-testing-board.org
www.swisstestingboard.org

ISTQB®
International Software Testing Qualifications Board

www.istqb.org

SECURITY TESTER

LEARNING OBJECTIVES

AS-1.1.1	(K2)	Understand the role of risk assessment in supplying information for security test planning and design and aligning security testing with business needs
AS-1.1.2	(K4)	Identify the significant assets to be protected, the value of each asset and the data required to assess the level of security needed for each asset
AS-1.1.3	(K4)	Analyze the effective use of risk assessment techniques in a given situation to identify current and future security threats
AS-1.2.1	(K2)	Understand the concept of security policies and procedures and how they are applied in information systems
AS-1.2.2	(K4)	Analyze a given set of security policies and procedures along with security test results to determine effectiveness
AS-1.3.1	(K2)	Understand the purpose of a security audit
AS-2.2.1	(K2)	Understand why security testing is needed in an organization, including benefits to the organization such as risk reduction and higher levels of confidence and trust
AS-2.3.1	(K2)	Understand how project realities, business constraints, software development lifecycle, and other considerations affect the mission of the security testing team
AS-2.4.1	(K2)	Explain why security testing goals and objectives must align with the organization's security policy and other test objectives in the organization
AS-2.4.2	(K3)	For a given project scenario, identify security test objectives based on functionality, technology attributes and known vulnerabilities
AS-2.4.3	(K2)	Understand the relationship between information assurance and security testing
AS-2.5.1	(K3)	Demonstrate the relationship between security test objectives and the strength of integrity of sensitive digital and physical assets
AS-2.6.1	(K4)	Analyze a given situation and determine which security testing approaches are most likely to succeed
AS-2.6.2	(K4)	Analyze a situation in which a given security testing approach failed, identifying the likely causes of failure
AS-2.6.3	(K3)	Identify the various stakeholders and explain the benefits of security testing for each stakeholder group
AS-2.7.1	(K4)	Analyze KPIs (key performance indicators) to identify security testing practices needing improvement and elements not needing improvement
AS-3.1.1	(K3)	Define the elements of an effective security test process
AS-3.2.1	(K4)	Analyze a given security test plan, giving feedback on strengths and weaknesses of the plan.
AS-3.3.1	(K3)	For a given project, design conceptual (abstract) security tests, based on a given security test approach, along with identified functional and structural security risks
AS-3.3.2	(K3)	Design test cases to validate security policies and procedures.
AS-3.4.1	(K2)	Understand the key elements and characteristics of an effective security test environment
AS-3.4.2	(K2)	Understand the importance of planning and approvals before performing any security test
AS-3.5.1	(K4)	Analyze security test results to determine the following: • Nature of security vulnerability • Extent of security vulnerability • Potential impact of security vulnerability • Suggested remediation course of action • Test reporting methods
AS-3.6.1	(K2)	Understand the importance of maintaining security testing processes given the evolving nature of technology and threats
AS-4.1.1	(K2)	Explain why security is best achieved within a lifecycle process
AS-4.1.2	(K2)	Describe the security-related activities needed in a given SDLC (e.g., agile, sequential)
AS-4.2.1	(K4)	Analyze a given set of requirements from the security perspective to identify deficiencies
AS-4.3.1	(K4)	Analyze a given design document from the security perspective to identify deficiencies
AS-4.4.1	(K2)	Understand the role of security testing during component testing
AS-4.4.2	(K3)	Design component level security tests (abstract) given a defined coding specification
AS-4.4.3	(K4)	Analyze the results from a given component level test to determine the adequacy of code from the security perspective
AS-4.4.4	(K2)	Understand the role of security testing during component integration testing
AS-4.4.5	(K3)	Design component integration security tests (abstract) given a defined system specification
AS-4.5.1	(K3)	Create an end-to-end test scenario for security testing which verifies one or more given security requirements and tests a described functional process

AS-4.5.2	(K3)	Define a set of acceptance criteria for the security aspects of a given acceptance test
AS-4.6.1	(K3)	Create an end-to-end security retest / regression test approach based on a given scenario
AS-5.1.1	(K2)	Understand the concept of system hardening and its role in enhancing security
AS-5.1.2	(K3)	Describe how to test the effectiveness of common system hardening mechanisms
AS-5.2.1	(K2)	Understand the relationship between authorization and authentication and how they are applied in securing information systems
AS-5.2.2	(K3)	Describe how to test the effectiveness of common authorization and authentication mechanisms
AS-5.3.1	(K2)	Understand the concept of encryption and how it is applied in securing information systems
AS-5.3.2	(K3)	Describe how to test the effectiveness of common encryption mechanisms
AS-5.4.1	(K2)	Understand the concept of firewalls and the use of network zones and how they are applied in securing information systems
AS-5.4.2	(K3)	Describe how to test the effectiveness of existing firewall implementations and network zones
AS-5.5.1	(K2)	Understand the concept of intrusion detection tools and how they are applied in securing information systems
AS-5.5.2	(K3)	Describe how to test the effectiveness of existing intrusion detection tool implementations
AS-5.6.1	(K2)	Understand the concept of malware scanning tools and how they are applied in securing information systems
AS-5.6.2	(K3)	Describe how to test the effectiveness of existing malware scanning tool implementations
AS-5.7.1	(K2)	Understand the concept of data obfuscation tools and how they are applied in securing information systems
AS-5.7.2	(K3)	Describe how to test the effectiveness of data obfuscation approaches
AS-5.8.1	(K2)	Understand the concept of security training as an SDLC activity and why it is needed in securing information systems
As-5.8.2	(K3)	Describe how to test the effectiveness of security training
AS-6.1.1	(K2)	Explain how human behavior can lead to security risks and how it impacts the effectiveness of security testing
AS-6.1.2	(K3)	Identify ways in which an attacker could discover key information about a target and explain how the environment could be protected.
AS-6.1.3	(K2)	Explain the common motivations and sources for performing computer system attacks
AS-6.1.4	(K4)	Analyze an attack scenario (attack performed and discovered)
AS-6.2.1	(K2)	Explain how security measures can be compromised by social engineering
AS-6.3.1	(K2)	Understand the importance of security awareness throughout the organization
AS-6.3.2	(K3)	Given certain test outcomes, define appropriate actions that can be taken to increase security awareness
AS-7.1.1	(K2)	Understand the need to revise security expectations and acceptance criteria as the scope and goals of a project evolve
AS-7.2.1	(K2)	Understand the importance of keeping security test results confidential and secure
AS-7.2.2	(K2)	Understand the need to create proper controls and data-gathering mechanisms to provide the source data for the security test status reports in a timely, accurate, and precise fashion (e.g., a security test dashboard)
AS-7.2.3	(K4)	Analyze a given interim security test status report to determine the level of accuracy, understandability, and stakeholder appropriateness
AS-8.1.1	(K2)	Explain the role of static and dynamic analysis tools in security testing
AS-8.2.1	(K4)	Analyze and document security testing needs to be addressed by one or more tools
AS-8.2.2	(K2)	Understand the issues with open source tools
AS-8.2.3	(K2)	Understand the need to evaluate the vendor's capabilities to update tools on a frequent basis to stay current with security threats
AS-9.1.1	(K2)	Understand the benefits of using security testing standards and where to find them
AS-9.1.2	(K2)	Understand the difference in applicability of standards in regulatory versus contractual situations
AS-9.2.1	(K2)	Understand the difference between mandatory (normative) and optional (informative) clauses within any standard
AS-9.3.1	(K2)	Understand where to learn of industry trends in information security

Swiss Testing Board

info@swiss-testing-board.org
www.swisstestingboard.org

ISTQB®
International Software
Testing Qualifications Board

www.istqb.org