

Table of Contents

Copyright Notice	2
Revision History	3
Table of Contents.....	4
Acknowledgements.....	8
0. Introduction	9
0.1. Purpose of this Syllabus	9
0.2. Business Outcomes.....	9
0.3. Examinable Learning Objectives and Cognitive Level of Knowledge	10
0.4. The Security Test Engineer Certification Exam	10
0.5. Accreditation.....	11
0.6. Handling of Standards	11
0.7. Level of Detail.....	11
0.8. How this Syllabus is Organized	11
1. Security Paradigms – 135 minutes (K3).....	13
1.1. Asset Security Levels.....	13
1.1.1. Assets and Their Corresponding Protection Level.....	14
1.1.2. Information Sensitivity and Security Testing.....	14
1.2. Security Audits.....	15
1.2.1. Security Audits and Security Testing	15
1.3. The Concept of Zero Trust.....	16
1.3.1. What is Zero Trust?	16
1.3.2. Zero Trust in Security Testing.....	17
1.4. Open-Source Software (OSS)	18
1.4.1. The Concept of OSS and its Impact on Security Testing.....	18
2. Security Test Techniques - 150 minutes (K3)	20
2.1. Applying Security Test Types According to a Test Context	20
2.1.1. Black-Box Testing, White-Box Testing, and Grey-Box Testing.....	20
2.1.2. Static and Dynamic Security Testing	21

2.2.	Applying Security Testing	23
2.2.1.	Addressing Security Risks in Test Design	23
2.2.2.	Reconciliation Testing and Recertification Testing	25
2.2.3.	Testing Identification, Authentication and Authorization	27
2.2.4.	Encryption.....	28
2.2.5.	Testing Protective Technologies.....	28
3.	The Security Test Process - 120 minutes (K3).....	32
3.1.	The Security Test Process.....	32
3.1.1.	ISTQB Security Test Process	32
3.1.2.	The Security Test Environment	35
3.2.	Designing Security Tests for Test Levels.....	35
3.2.1.	Security Test Design at Component Test Level.....	36
3.2.2.	Security Test Design at the Component Integration Level.....	38
3.2.3.	Security Testing in System Testing and Acceptance Testing	39
4.	Security Testing Standards and Best Practices - 195 minutes (K3).....	41
4.1.	Introduction to Standards and Best Practices	41
4.1.1.	Standards and Best Practices	42
4.2.	Apply Important Standards and Best Practices for Security Testing	43
4.2.1.	Industry Standards for Security Testing.....	43
4.3.	Leveraging Security Testing Standards and Best Practices	47
4.3.1.	Mandatory Application of Standards and Best Practices	47
4.3.2.	Voluntary Application of Standards and Best Practices	48
4.3.3.	Test Oracles Extracted from Standards and Best Practices	48
4.3.4.	Advantages and Disadvantages of Leveraging Security Testing Standards and Best Practices.....	48
5.	Adjusting Security Testing to the Organizational Context - 195 minutes (K4)	50
5.1.	The Impact of Organizational Structures in the Context of Security Testing	50
5.1.1.	Analyze a given organizational context and determine which specific aspects to consider for security testing	50
5.2.	The Impact of Regulations on Security Policies and How to Test Them.....	53
5.2.1.	The Impact of Governmental Regulations on Security Regulations.....	53

5.3.	Analyzing an Attack Scenario	56
5.3.1.	Common Attack Scenarios	56
6.	Adjusting Security Testing to Software Development Lifecycle Models - 165 minutes (K4).....	63
6.1.	The Effects of Different Software Development Lifecycle Models on Security Testing	63
6.1.1.	Sequential Development Models	65
6.1.2.	Agile Software Development	66
6.1.3.	The DevOps Methodology	68
6.2.	Security Testing During Operations and Maintenance.....	69
6.2.1.	Security Regression Testing and Confirmation Testing	69
7.	Security Testing as Part of an Information Security Management System - 105 minutes (K3)	71
7.1.	Acceptance Criteria for Security Testing.....	71
7.2.	Input for an Information Security Management System (ISMS)	73
7.3.	Improving an ISMS by Adjusting Security Testing	74
7.3.1.	Improving the Holistic View of an ISMS	74
7.3.2.	Improving Measurability within an ISMS	76
8.	Reporting Security Test Results - 135 minutes (K3)	77
8.1.	Security Test Reporting	77
8.2.	Identifying and Analyzing Vulnerabilities.....	78
8.3.	Close Identified Vulnerabilities.....	80
8.3.1.	Hiding a Vulnerability	80
8.3.2.	Avoiding a Vulnerability	81
9.	Security Testing Tools - 90 minutes (K3)	83
9.1.	Categorization of Security Testing Tools	83
9.1.1.	White-box Security Testing Tools	84
9.1.2.	Black-box Security Testing Tools	84
9.1.3.	Grey-box Security Testing Tools	84
9.1.4.	Static Security Testing Tools	84
9.1.5.	Dynamic Security Testing Tools	85
9.1.6.	Considerations for Selecting Security Testing Tools	86
9.2.	Applying Security Testing Tools.....	87
9.2.1.	Understand the Usage and Concepts of Static Security Testing Tools	87

9.2.2. Understand the Usage and Concepts of Dynamic Security Testing Tools	87
10. References.....	89
Appendix A – Learning Objectives/Cognitive Level of Knowledge	94
Level 1: Remember (K1).....	94
Level 2: Understand (K2).....	94
Level 3: Apply (K3)	95
Level 4: Analyze (K4).....	95
Appendix C – Release Notes.....	100
Appendix D – Security Testing Domain-Specific Terms.....	101
Index	103