Sample Exam – Answers

Sample Exam set notation of exam paper
Version 1.0

ISTQB® Security Test Engineer Syllabus Specialist Level

Compatible with Syllabus version 1.0

International Software Testing Qualifications Board

Version 1.0

Released release date

Copyright Notice

Document Responsibility

The ISTQB® Examination Working Group is responsible for this document.

This document is maintained by a core team from ISTQB® consisting of the Syllabus Working Group and Exam Working Group.

Acknowledgements

This document was produced by a core team from the ISTQB®: The core team thanks the Exam Working Group review team, the Syllabus Working Group and the National Boards for their suggestions and input.

This document is maintained by a core team from ISTQB® consisting of the Syllabus Working Group and Exam Working Group.

Revision History

Sample Exam – Answers Layout Template used:	Version 2.6	Date: September 29, 2021

Version	Date	Remarks
1.0	2024-09-10	Final version for GA approval

Table of Contents

Introduction

Purpose of this document

The example questions and answers and associated justifications in this sample exam have been created by a team of subject matter experts and experienced question writers with the aim of:

- Assisting ISTQB® Member Boards and Exam Boards in their question writing activities
- Providing training providers and exam candidates with examples of exam questions

These questions cannot be used as-is in any official examination.

Note, that real exams may include a wide variety of questions, and this sample exam ***is not*** intended to include examples of all possible question types, styles or lengths, also this sample exam may both be more difficult or less difficult than any official exam.

Instructions

In this document you may find:

- Answer Key table, including for each correct answer:
  - K-level, Learning Objective, and Point value
- Answer sets, including for all questions:
  - Correct answer
  - Justification for each response (answer) option
  - K-level, Learning Objective, and Point value
- Additional answer sets, including for all questions [does not apply to all sample exams]:
  - Correct answer
  - Justification for each response (answer) option
  - K-level, Learning Objective, and Point value

- *Questions are contained in a separate document*

Answer Key

Question Number (#)	Correct Answer	LO	K-Level	Points
1	A	STE 1.1.1	K2	1
2	A	STE 1.1.2	K2	1
3	B	STE 1.2.1	K2	1
4	A	STE-1.3.1	K3	1
5	A, C	STE-1.3.2	K3	1
6	C	STE 1.4.1	K3	1
7	B, C	STE-2.1.1	K2	1
8	C	STE-2.1.2	K2	1
9	A	STE-2.2.1	K3	1
10	B, C	STE-2.2.2	K2	1
11	C	STE-2.2.3	K2	1
12	C	STE-2.2.4	K2	1
13	A	STE-2.2.5	K2	1
14	B	STE-3.1.1	K2	1
15	C	STE-3.1.2	K2	1
16	B	STE-3.2.1	K2	1
17	C	STE-3.2.2	K3	1
18	A	STE-3.2.3	K3	1
19	A	STE-4.1.1	K3	1
20	C, E	STE-4.2.1	K3	1

Question Number (#)	Correct Answer	LO	K-Level	Points
21	D	STE 4.3.1	K2	1
22	A	STE 4.3.2	K3	1
23	B, C	STE 5.1.1	K3	1
24	A	STE-5.2.1	K3	1
25	D	STE-5.3.1	K4	2
26	A	STE 5.3.1	K4	2
27	A	STE 6.1.1	K2	1
28	D, E	STE 6.1.2	K4	2
29	C	STE 6.2.1	K3	1
30	C	STE 6.2.2	K2	1
31	B, D	STE 7.1.1	K2	1
32	A, C	STE 7.2.1	K2	1
33	A	STE 7.3.1	K3	1
34	A	STE 7.3.2	K2	1
35	B	STE 8.1.1	K2	1
36	A, D	STE 8.2.1	K3	1
37	A, D	STE 8.3.1	K3	1
38	A	STE 9.1.1	K3	1
39	A	STE-9.2.1	K2	1
40	A	STE-9.2.2	K2	1

3

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
1	a	a) Is correct: integrity seeks to prevent data from modification or deletion by any unauthorized party and is measured by the degree to which an asset allows only authorized access and modification. b) Is not correct: see above. c) Is not correct: see above. d) Is not correct: its availability.	STE-1.1.1	K2	1
2	a	a) Is correct: Confidentiality in security testing ensures that sensitive data is accessed only by authorized users. Security testing verifies that access controls mechanisms are effective, thereby preventing unauthorized access to confidential information. b) Is not correct: it is about integrity. c) Is not correct: it is about availability and quick recovery mechanisms after an incident. d) Is not correct: it is about the organization's response to incidents	STE-1.1.2	K2	1
3	b	a) Is not correct. This is a description of security testing in general. b) Is correct. Security audit evaluates an organization's security processes and infrastructures and is a type of static test technique c) Is not correct. Although the goal is ok, the audit focus on processes and controls d) Is not correct. Audits focus on processes and controls	STE-1.2.1	K2	1

4	a	a) Is correct: all users are treated as untrusted and are required to authenticate and authorize before they can access any resources b) Is not correct: A traditional network is one in which all devices and users are trusted by default. c) Is not correct: A Zero Trust architecture refers to a security model that doesn't inherently trust anything inside the network. d) Is not correct: A Zero Trust system ensures that no one can access data unless they have the proper credentials.	STE-1.3.1	K2	1
5	a, c	a) Is correct: Zero Trust verifies user identity, privileges as well as device identity and security for each access. Logins and connections time out periodically, forcing users and devices to be continuously re-verified. b) Is not correct: Non-human accounts must also be monitored c) Is correct: granted access to the resources must be logged permanently and as time-stamped record. d) Is incorrect: Encryption and restriction accesses of assets are based on organizational policies. e) Is not correct: Limit access controls to specific applications, resources, data, and assets, rather than the broader network.	STE-1.3.2	K3	1
6	c	a) Is not correct: Open-source software is software developed and maintained via open collaboration b) Is not correct: Open-source software is software developed and maintained via open collaboration c) Is correct: OSS is built on open source-code is open to be, used, modified, and shared by anyone. d) Is not correct: because the tool is free although you may have development costs in customizing the tool for your needs.	STE-1.4.1	K2	1

7	b, c	a) Is incorrect because source code is not available in a pre-production environment and it's not possible to discover all defects b) Is correct because this is a best practice to do black-box vulnerability scanning before the deployment c) Is correct because this is also a best practice to check that all entry points are not vulnerable d) Is not correct because, like a), source code is not available in a pre-production environment e) Is not correct because, like a), source code is not available in a pre-production environment	STE 2.1.1	K2	1
8	c	a) Is not correct because security coding rules checking must be done after security requirement ruleset is complete b) Is not correct because dynamic tests are executed c) Is correct because there are only static checks, and they are well-ordered d) Is not correct because dynamic tests are executed	STE-2.1.2	K2	1
9	a	a) Is correct because it covers the main scenarios for the functional security specified in the requirement b) Is not correct because it tests only valid tests c) Is not correct because it tests only error conditions d) Is not correct because it expands into penetration testing	STE-2.2.1	K3	1

10	b, c	a) Is not correct because modifications of roles and rights must be reviewed b) Is correct because rights and roles set or modified must be reviewed c) Is correct because modifications of roles and rights must be verified (correctness) and validated (aligned with the person needs) d) Is not correct because we don't know what modifications are applied to the different accounts. e) Is not correct because we have to check application access revoke as well.	STE-2.2.2	K2	1
11	C	a) Is not correct because it is not looking at access rights. b) Is not correct because system resource utilization is not a consideration. c) Is correct because it verifies that the user is legitimate and authorized d) Is not correct common credential verification should not be used – each individual should have unique credentials.	STE-2.2.3	K2	1
12	C	a) Is not correct because a minimum of 2048 bits should be used. b) Is not correct because the random algorithm is easy to crack. c) Is correct because verifying setup, parameters, and implementation reduces vulnerabilities and strengthens security. d) Is not correct because log files must not store any sensitive information	STE-2.2.4	K2	1

13	A	a) Is correct because there are security performance reports and metrics available that can be used to determine if you have achieved the right level of hardening. b) Is not correct because strong authentication is just one aspect of hardening. c) Is not correct because equilibrium is not needed. The more critical areas may warrant better hardening. d) Is not correct. because there is the danger of the hacker not telling you what is found.	STE-2.2.5	K2	1
14	B	a) Is not correct because this has already been done with the creation of the high-level tests. b) Is correct because the use of the high-level tests to create the manual tests and perform the execution is part of the security test implementation c) Is not correct because it will occur after the tests have been executed d) Is not correct because this has already been done with the creation of the high-level tests.	STE-3.1.1	K2	1
15	C	a) Is not correct because the system doesn't need to be and probably shouldn't be connected b) Is not correct because it may be useful, but it is not a main characteristic c) Is correct because the closer the test environment mimics production, the more valid the testing will be. This is particularly true when it comes to access rights and delegation settings. d) Is not correct because it includes plug-ins that are not in production which could result in both false positives and false negatives from the testing	STE-3.1.2	K2	1

16	B	a) Is not correct because warnings do not necessarily require a fix b) Is correct because from a security testing standpoint, compiler warnings indicate potential issues that could lead to security vulnerability c) Is not correct because it may be true, but it is not related to security testing d) Is not correct because it may be true, but it is not related to security testing	STE-3.2.1	K2	1
17	C	a) Is not correct because component integration testing is not the sum of the individual components. b) Is not correct because the testing should not be limited to just the interfaces and the original components. c) Is correct because new vulnerabilities may be present with the integrated components and new testing areas are likely to be available d) Is not correct because security risks are likely to be increased, not decreased.	STE-3.2.2	K2	1
18	a	a) Is correct. This is the best security practice compared to the others b) Is not correct because of the word “several”. The number of attempts is not quantified. c) Is not correct because of the word “several”. The number of attempts is not quantified. d) Is not correct because it would definitely not be a good security practice to store passwords not encrypted in notepad	STE-3.2.3	K3	1

19	a	a) Is correct, because standards are approved by a recognised body of knowledge b) Is not correct, because industry standards and de-facto-standards not mandatory c) Is not correct as standards are not mandatory. d) Is not correct as there is no correlation between level of detail and best practices, i.e. there exist very detailed best practices.	STE-4.1.1	K3	1
20	c, e	a) is not correct as CWEs do not contain any test cases (abstraction layer CVE is missing) b) Is not correct as CWEs do not contain exploits (abstraction layer CVE is missing) . c) Is correct as CWE clusters different attack types, CWSS prioritize them and CVSs are specific vulnerabilities for a given CWE. d) Is not correct as CWSSs do not contain test cases (abstraction layer CVE is missing) e) Is correct as CVE leaves it to the security tester to derive specific test cases	STE-4.2.1	K3	1
21	d	a) Is not correct, as context parameters might have an impact on the app behavior b) Is not correct, as test oracles for apps without a specific context can efficiently be used for security testing c) Is not correct, as test oracles for apps without a specific context can efficiently be used for security testing d) Is correct: If all parameters of an app are standard, test oracles can directly be reused for security testing	STE-4.3.1	K2	1

22	a	a) Is correct as a consistent nomenclature enables easier communication (1a), expert knowledge reuses security expert knowledge (2b) benchmarking easily demonstrates effectiveness of applied security testing activities (3d) and holistic security overview by a group of experienced experts can doublecheck completeness of security testing activities. b) 3c is not correct (Benchmarking does not necessarily give any evidence for completeness) 4d is not correct (holistic security overview does not give eny evidence for effectiveness. c) 1d is not correct (nomenclature does not give any evidence for effectiveness), 2a is not correct (expert knowledge does not necessarily simply communication) 3b is not correct (Benchmarking does not nessarily allow for reusing expert knowledge) d) 1b is not correct (nomenclature does not reuse security expert knowledge), 2d is not correct (expert knowledge does not necessarily give any evidence for effectiveness), 3a is not correct (benchmarking does not allow for an easier communication)	STE-4.3.2	K3	1
23	b, c	a) Is not correct: To bring the security test activities to a point of closure so the tests can be maintained and performed on a regular basis to support any new security requirements and/or detect new threats b) Is correct, since the company is highly dependent on their suppliers, there is an increased chance of having success by faking a supplier's id c) Is correct, since the company is highly dependent on their suppliers, billings from a supplier might be more important for the accounting than others d) Is not correct, because it does not take advantage of the organizational context. e) Is not correct, because it does not take advantage of the organizational context	STE-5.1.1	K3	1

24	a	a) Is correct, aviation is strong regulated which has to be considered by security tester b) Is not correct. Even though this has to be tested, the test aims more to a functional requirement and is not scope of security testing. If there might exist negativ side effects, this has to tested instead of being ignored c) Is not correct as time/budget is no constraint in any regulated context. d) Is not correct, because it does not take advantage of the organizational context and does give any guidance when focusing on test activities	STE-5.2.1	K3	1
25	d	a) Is not correct, as continuing testing activities can blur traces of an actual security incident. Also reporting only after finishing all testing activities might be too late in case of a serious incident b) Is not correct, as an attacker could also be an insider. Also see a) why continuing testing is not a valid solution c) Is not correct, Stopping a system might cause loss of traces in case of an incident. While this might be a valid solution in some cases, a security tester has not the authority to decide this on his own d) Is correct, as a company should have working Incident Response Mechanisms and after reporting an incident, processes should take place in order to investigate the reported incident	STE-5.3.1	K4	2
26	a	a) As mentioned in the syllabus b) Not all attacks are starting with social engineering c) Exploitation/gaining access is done after information gathing (e.g. done by social engineering) d) The step of getting access is missing, so no attack is done	STE-5.3.1	K4	2
27	a	a) Correct as mentioned in the syllabus b) Only static security testing activities will not be able to find all vulnerabilities c) SAST and DAST can be performed but should be supplemented with extra security test activities and verifications d) There is no documented need to keep security testing in sync with manual testing	STE-6.1.1	K2	1

28	d, e	a) Is correct as in the syllabus b) Is not correct: Waterfall model activities have to be planned up front which may cause needed changes during execution c) Is not correct: Most organization using DevOps have a security team verifying in production during operation. It is not given that the DevOps team is involved d) Is correct: Both software development models enable for ad hoc changes in tasks and the use for enabling teams when needed e) Is correct: The Agile development model opens for ad hoc plan changes when needed	STE-6.1.2	K4	2
29	c	a) Incorrect as by the glossary b) Incorrect, there is no proof for such statement c) Correct, as mentioned in the syllabus d) Incorrect	STE-6.2.1	K3	1
30	c	a) Is not correct as by the glossary b) Is not correct, there is no proof for such statement c) Is correct, as mentioned in the syllabus d) Is not correct	STE-6.2.2	K2	1
31	b, d	a) Is not correct as a test report must contain all information that are necessary to understand the results. It does not need any background about the specific tester. b) Is correct as project specific acceptance criteria are not necessarily part of OWASP Top-10. c) Is not correct as OWASP lists Best Practice vulnerabilities, but acceptance criteria are dependent on a specific business context. d) Is correct, as a pentest has a black-box view on that system and can not test any white-box aspects. e) Is not correct, as there exist many different context specific security code style guides, which can not be reflected by one generic OWASP.	STE-7.1.1	K2	1

32	a, c	a) Is correct as security testing without any surrounding framework and regular iterations does not generate any systematically added value. b) Is not correct as a yearly frequency can be too low for very critical systems and it can be too high for a nice-to-have-tool. c) Is correct as security testing helps identifying vulnerabilities as early as possible d) Is not correct as day-to-day communicated vulnerabilities might be irrelevant for a specific context (e.g. no internet connection) . e) Is not correct, as there might exist identified vulnerabilities that are irrelevant for a specific context or do not need any remediation ever as there exist other mitigating systems (e.g. a specific firewall). On the other side there might exist vulnerabilities, for which the 6 months timeframe might be too long for identified and exploitable vulnerabilities with high or critical severity.	STE-7.2.1	K2	1
33	a	a) Is correct as adding additional test objects to a test plan can be used for identifying additional weaknesses (1c), adding additional test approaches can be used for bringing in additional insights into a given system (2a) and improved test coverage while sticking on given test objects and test approaches can be used for identifying additional weaknesses b) Is not correct, as 1b is not correct (additional test objects are not known to the ISMS) and 2d is not correct (additional test approaches do not make any IT system more secure. . c) Is not correct, as 4b is wrong (increase automation of security test execution does not increase an ISMS in any way, neither does it identify any additional weaknesses. d) Is not correct, as 1d is wrong (additional test objects do not make any IT system more secure), 2c is wrong (additional test approaches do not identify new components), and 4a is wrong (increase automation of security test execution does not increase an ISMS in any way, neither does it generate new insights into a given system)	STE-7.3.1	K3	1

34	a	a) The right answer is A (explained in Syllabus) b) All Security testing generates quantifiable insights into the security of a system that can be used to measure ISMS effectiveness. c) The number of security tests do not correlate with quality of security. d) The effectiveness of an ISMS is better the more security testing techniques are used.	STE-7.3.2	K2	1
35	b	a) Is not correct as the name of the security tester and the test frame is irrelevant b) Is correct as the test environment, pre-set preconditions of the executed tests, the used test data, the procedure of test execution as well as the detected behavior can represent confidential data. c) Is not correct as the list of named developers, the identified software development method as well as the development tools are irrelevant. d) Is not correct as the coding functions as well as the functional test coverage is irrelevant.	STE 8.1.1	K2	1
36	a, d	a) Is correct as an identified vulnerabilities still might miss some information before mitigation. b) Is not correct as it is not the task of the security tester to do an effort estimation for an identified vulnerability. c) Is not correct as it is not the task of the security tester to create a design on how to mitigate an identified vulnerability. d) Is correct as it is important to doublecheck that the identified vulnerability can be exploited on production e) Is not correct as it is not the task of the security engineer to immediately repair any finding.	STE 8.2.1	K3	1
37	a, d	a) Is correct as switching off a specific feature can mitigate an identified risk. b) Is not correct as it depends on the type of vulnerability if this technique is successful. c) Is not correct as you can not expect all vulnerabilities to be automatically blocked in a Web Application Firewall. d) Is correct as adding security controls can reduce risk e) Is not correct as deleting vulnerabilities can be very expensive and time consuming, so other opportunities should be analyzed in advance to mitigate risk much earlier.	STE 8.2.2	K3	1

38	a	a) Is correct. SCA is a very fast check on the components in use and should be run before any other checks. b) Is not correct. Although SAST ensures that no security vulnerabilities remain unknown it is focused on the application code c) Is not correct. This requires the application to be running. d) Is not correct. This requires the application development to be in a later stage	STE 9.1.1	K3	1
39	a	a) Is correct. DAST is a dynamic scanner b) Is not correct. SA is not dynamic c) Is not correct. SCA is a static testing method d) Is not correct. SAST	STE 9.2.1	K2	1
40	a	a) Is correct as code can be analyzed b) Is not correct. A design can be reviewed manually c) Is not correct. The code can bu the service cannot d) Is not correct. Processes can be monitored but not statical analysed	STE 9.2.2	K2	1

4