Sample Exam – Answers

Sample Exam set A
Version 1.1

ISTQB® Security Testing Syllabus Specialist

Compatible with Syllabus version 2016

International Software Testing Qualifications Board

Version 1.1 Released June 8, 2021

Copyright Notice

Document Responsibility

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

Acknowledgements

This document was produced by a core team from the ISTQB®: Security Testing team

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 2.5	Date: Maj 21, 2021

Version	Date	Remarks
1.1	June 8, 2021	Update of Copyright Notice Update of layout
1.0	March 15, 2016	First version

Table of Contents

Copyright Notice 2
Document Responsibility 2
Acknowledgements 2
Revision History 3
Table of Contents 4
Introduction 6
Purpose of this document 6
Instructions 6
Answer Key 7
Answers 8
1 8
2 8
3 8
4 8
5 9
6 9
7 9
8 9
9 10
10 10
11 10
12 11
13 11
14 11
15 12
16 12
17 12
18 13
19 13
20 13
21 13
22 14
23 14
24 14
25 15
26 15
27 15
28 15
29 16
30 16
31 16
32 16
33 17
34 17
35 17
36 18
37 18
38 18
39 19
40 19
41 19
42 20
43 20

44 20
45 20

Introduction

Purpose of this document

The sample questions and answers and associated justifications in this sample exam set 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.

These questions cannot be used as-is in any official examination, but they should serve as guidance for question writers. Given the wide variety of formats and subjects, these sample questions should offer many ideas for the individual Member Boards on how to create good questions and appropriate answer sets for their examinations.

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	b	-	-	1
2	c	-	-	3
3	c	-	-	1
4	b	-	-	3
5	a	-	-	1
6	c	-	-	1
7	b	-	-	2
8	c	-	-	2
9	d	-	-	3
10	c	-	-	2
11	b	-	-	2
12	b	-	-	3
13	a	-	-	2
14	c	-	-	1
15	a	-	-	1
16	b	-	-	3
17	a	-	-	1
18	b	-	-	2
19	c	-	-	3
20	b	-	-	1
21	c	-	-	2
22	c	-	-	3
23	a	-	-	2
24	d	-	-	2
25	a	-	-	2
26	c	-	-	1
27	c	-	-	2
28	c	-	-	1
29	b	-	-	2
30	b	-	-	1
31	b	-	-	2
32	c	-	-	1
33	a	-	-	1
34	d	-	-	2
35	c	-	-	1
36	c	-	-	3
37	d	-	-	2
38	b	-	-	1
39	c	-	-	1
40	c	-	-	3
41	a	-	-	1
42	a	-	-	3
43	c	-	-	1
44	b	-	-	1
45	b	-	-	1

Answers

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
1	b	a) Is not correct b) Is correct. As keeping the patch updates current on the system is one of the purposes of a security audit. The others are good practices, but not the purpose of the security audit c) Is not correct d) Is not correct	-	-	1
2	c	a) Is not correct. Need to be informed, but the information needs to come from the federal and local agencies b) Is not correct. Need to be informed, but the information needs to come from the federal and local agencies c) Is correct. As this is the source of the guidelines. The guidelines may change so it is important to keep the communications channels open with these folks d) Is not correct. Need to be informed, but the information needs to come from the federal and local agencies	-	-	3
3	c	a) Is not correct. As this would not be an expected results b) Is not correct. Because these controls will be encouraged c) Is correct. When this policy is implemented, non-conforming devices will be removed until they conform d) Is not correct. Because access will be controlled, not severely limited	-	-	1
4	b	a) Is not correct. Because the static analysis should be over the code, if anything b) Is correct. You should analyze the results of a security test to see if the policies and procedures have been followed and are effective c) Is not correct. Because the focus should not just be on current threats and attacks, but also on configurations, etc. d) Is not correct. Because the focus is not just on the emerging threats	-	-	3

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
5	a	a) Is correct. Per the syllabus b) Is not correct. Because this information would probably not be helpful c) Is not correct. Because the backup would likely be out of date and the information was not necessarily corrupted, but rather stolen or viewed d) Is not correct. Because, although this may help point to areas where testing was not sufficient, it will not support the organization’s defense of legal actions	-	-	1
6	c	a) Is not correct b) Is not correct c) Is correct. Security testing is a part of the larger area of information assurance d) Is not correct	-	-	1
7	b	a) Is not correct. Because 3 is functional rather than security-related (unless it locks them out, but we do not know that from this description) b) Is correct. Because all of these are valid security objectives c) Is not correct. Because 6 and 7 are both functional rather than specific security requirements d) Is not correct. Because 6 and 7 are both functional rather than specific security requirements	-	-	2
8	c	a) Is not correct. Is reasonable concerns, but you do not know when or how the test objectives will be defined, so this may be controllable b) Is not correct. Is always a possibility and may be the right thing to do in this case, but there has been no indication that outsourcing will occur at this time c) Is correct. per the syllabus as this is a common problem when the objectives are broadly defined d) Is not correct. Is reasonable concerns, but you do not know when or how the test objectives will be defined, so this may be controllable	-	-	2

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
9	d	a) Is not correct. At this point although they might be useful if you have trouble getting funding when you work to implement the policy b) Is not correct. Because you need an overall policy before you define the approach c) Is not correct. At this point although they might be useful if you have trouble getting funding when you work to implement the policy d) Is correct. At this point, the organization needs a high-level policy and plan to move forward. Without this policy, the testing may continue to be sporadic and high-level support and funding will be difficult	-	-	3
10	c	a) Is not correct. Will not be involved, this is not usually their primary benefit b) Is not correct. Will not be involved, this is not usually their primary benefit c) Is correct. The business customers will be most concerned with protection from fraudulent access as it is their data that is vulnerable d) Is not correct. Will not be involved, this is not usually their primary benefit	-	-	2
11	b	a) Is not correct. Because this has already been done with the creation of the conceptual tests b) Is correct. The use of the conceptual tests to create the manual tests and perform the execution is part of the security test implementation c) Is not correct. Will occur after the tests have been executed d) Is not correct. Because this has already been done with the creation of the conceptual tests	-	-	2

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
12	b	a) Is not correct. Might be needed but that is not one of the minimum requirements and may already be understood in the roles and responsibilities section b) Is correct. Per the syllabus c) Is not correct. Because the standards might be referenced but not included in the plan d) Is not correct. Because this level of detail does not belong in the plan and the individual testers should not be contacted during a breach	-	-	3
13	a	a) Is correct b) Is not correct. Because of the word "several" c) Is not correct. Because of the word "several" d) Is not correct. Because this would definitely not be a good security practice	-	-	2
14	c	a) Is not correct. Because the system do not need to be and probably should not be connected b) Is not correct. May be useful, but 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	-	-	1

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
15	a	a) Is correct. While some tools are quite good and effective for testing, they may be prohibited by some countries and some organizations b) Is not correct. Because there is always a danger of deploying a sub-optimal tool to deal with a crisis. A fast-track approval process makes sense, but a complete bypass is risky c) Is not correct. Because there may be unknown risks from tools and it is better to do the due diligence in tool selection rather than deal with the consequences of a poorly selected tool d) Is not correct. Because there may be unknown risks from tools and it is better to do the due diligence in tool selection rather than deal with the consequences of a poorly selected tool	-	-	1
16	b	a) Is not correct. Because the defect should not be publicized in the stakeholder report b) Is correct. The first priority is to see if the problem exists in the production version. The defect should be documented only in a secure defect tracking system since the problem may exist in production. Since one XSS issue was found, there may be others so continued testing is warranted c) Is not correct. Because while further testing is needed, notification is critical d) Is not correct. Because of the stakeholder reporting	-	-	3
17	a	a) Is correct. The checking should be done as soon as the code is written b) Is not correct c) Is not correct d) Is not correct	-	-	1

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
18	b	a) Is not correct. Although it is important that the documented requirements be protected from those who do not need to know b) Is correct c) Is not correct. Because although they may be refined at the design level, they should be initially captured during the requirements definition phase d) Is not correct. Because security requirements also need to include secure coding practices, etc.	-	-	2
19	c	a) Is not correct. Because the fix should fix the problem b) Is not correct. Because there should be no impact to usability (unless you are the hacker!) c) Is correct. It is likely that this level of checking will slow down the system because it will have to check on each screen change d) Is not correct. Because the fix should fix the problem	-	-	3
20	b	a) Is not correct. Because warnings do not necessarily require a fix b) Is correct. From a security testing standpoint, compiler warnings indicate potential issues that could lead to security gaps c) Is not correct. Is not related to security testing d) Is not correct. Is not related to security testing	-	-	1
21	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. 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	-	-	2

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
22	c	a) Is not correct. Has more than the minimum number b) Is not correct. Has more than the minimum number c) Is correct. As this has one test for SQL injection and one for a valid input. This is the minimum number of tests d) Is not correct. It does not have enough tests because it does not test the valid input. It would be advisable to do more testing on the various characters that can support SQL injection, but this question is asking to apply EP and get the minimum number of test cases	-	-	3
23	a	a) Is correct. As it covers the main scenarios for the functional security specified in the requirement b) Is not correct. Tests only on the valid tests c) Is not correct. Tests only the error conditions d) Is not correct. Expands into attack testing as well as functional testing	-	-	2
24	d	Consider: • 7 is tempting and would be logical, but it is not specified in the requirement • The others are not true. Because they do not contain the proper criteria • 2 Is not true, where 3 is true • 4 Is not true, where 5 is true Thus: a) Is not correct b) Is not correct c) Is not correct d) Is correct. Because it provides the acceptance criteria based on the requirement	-	-	2

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
25	a	a) Is correct. 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	-	-	2
26	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. It verifies that the user is legitimate and authorized d) Is not correct. Because common credential verification should not be used – each individual should have unique credentials	-	-	1
27	c	a) Is not correct. Because a minimum of 768 bits should be used b) Is not correct. Because the random algorithm is easy to crack c) Is correct. Per the syllabus d) Is not correct. Because WEP protocols should be left in place, not removed	-	-	2
28	c	a) Is not correct. Because network zones do not focus on size of data b) Is not correct. Network zones are parts of the configuration of the firewall and define the authorized flow of data between networks c) Is correct. Per the syllabus d) Is not correct. Because the firewall blocks the traffic, not the network zone	-	-	1

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
29	b	a) Is not correct. Might be useful, but will not be as effective in making sure the tool will work for the future as well as the present b) Is correct. Because these tests can be used to add new intrusive specifications, which were, formerly considered to be authorized traffic c) Is not correct. Might be useful, but will not be as effective as B in making sure the tool will work for the future as well as the present d) Is not correct. Is true for the usage, but not for the testing	-	-	2
30	b	a) Is not correct. May be correct depending on the particular focus of the tool, but is not a main disadvantage b) Is correct. The malware tool can only detect malware that it already knows about c) Is not correct. The tools are normally easy to run d) Is not correct. Because the tools provide the ability to update themselves with new findings and to produce reports	-	-	1
31	b	a) Is not correct. Because it is generally not feasible because of the amount of data and time it would take b) Is correct. Per the syllabus. A brute force or dictionary attack can be used to see if personal information is still accessible c) Is not correct. Because this is more of an anonymizing exercise. Also, the field length might be limited so this may corrupt the data d) Is not correct. Because we are not trying to stress test the database itself	-	-	2
32	c	a) Is not correct b) Is not correct c) Is correct. It is the people and their behavior that is the weakest link d) Is not correct	-	-	1

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
33	a	a) Is correct. This information could be used to determine approval chains for invoice approvals, which could then be used to create and approve fake invoices if the accounting system can be hacked b) Is not correct. Because the birth date should not be used in any employee information such as a password c) Is not correct. Because the company intranet should be behind the firewall with other protected information d) Is not correct. Because this information is unlikely to be useful to a hacker	-	-	1
34	d	a) Is not correct. This could be a dangerous assumption b) Is not correct. Because the hacker still has access to the system c) Is not correct. May be true, but re-running the same tests is not going to help with this issue d) Is correct. This is your biggest point of concern	-	-	2
35	c	a) Is not correct. Is more likely to occur with an external attacker b) Is not correct. Is more likely to occur with an external attacker c) Is correct. The biggest threat here is that the external protections are useless because the attacker is already inside the system d) Is not correct. Is not the most likely attack – generally, internal users are after information they can sell or can use to embarrass the company	-	-	1

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
36	c	a) Is not correct. would be the next likely paths to pursue since it is possible this is an internal attack (D) or that the attacks are separate and the birthdate information might provide some information as to who has been near it b) Is not correct. Might be pursued, but it would be easier to just ask the sys admin who would know the dog's name c) Is correct. It is the best place to start because it appears that this might have been where the problem originated. If C does not find anything d) Is not correct. Would be the next likely paths to pursue since it is possible this is an internal attack or that the attacks are separate and the birthdate information might provide some information as to who has been near it	-	-	3
37	d	a) Is not correct. Because this is exactly what security testers should be doing b) Is not correct. Because management permission should always be obtained prior to testing, not afterward c) Is not correct. Should be the next step to ensure the developers are coding correctly and using all available tools to check for this type of issue d) Is correct. The first priority is to see if the vulnerability is in the production code and get the problem fixed immediately	-	-	2
38	b	a) Is not correct. Because everyone does not need to know everything b) Is correct. Stakeholders often have to make business decisions regarding the security risk level that is acceptable and any necessary mitigation plans c) Is not correct. Because a manual-based risk mitigation plan is not feasible and the users probably would not be implementing this anyway d) Is not correct. Because expectations should change	-	-	1

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
39	c	a) Is not correct. Because of the need to tightly control access to the results b) Is not correct. Because only limited parts of the report should be made available to the developers to improve their coding. Likewise, limited parts should be made available to infrastructure people to fix any infrastructure issues that may have been found c) Is correct. The results from security tests should be kept confidential and access to the results should be tightly controlled. This is because the outcome of the tests often identify weaknesses in the current system under test and often the same issues exist with the production system d) Is not correct. Is true, but is not the most important aspect	-	-	1
40	c	a) Is not correct. Because the details should not be in the summary b) Is not correct. Because the information should not be recorded only at the end of the report c) Is correct. The risk impact should be described in the summary and detailed later in the report by discussing specific vulnerabilities d) Is not correct. Because this is an important part of the report	-	-	3
41	a	a) Is correct b) Is not correct. Because there are both dynamic and static analysis security tools c) Is not correct. Because memory leaks are detected by the general dynamic analysis tools, not the security specific ones d) Is not correct. Because this is true of all static analysis tools	-	-	1

Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
42	a	a) Is correct. As both of these techniques are used to test firewalls b) Is not correct. Because the goal is to prevent the attack rather than let it get through the firewall c) Is not correct. Because the goal is to prevent the attack rather than let it get through the firewall d) Is not correct. Because software component hardening will help the individual software components, but not the firewall and its implementation	-	-	3
43	c	a) Is not correct. Because there is no vendor b) B incorrect. Because there is no vendor c) Is correct. The GNU license is free and it is an open source community so there is no vendor d) Is not correct. Because the tool is free although you may have development costs in customizing the tool for your needs	-	-	1
44	b	a) Is not correct. Because security standards may be mentioned in the project goals and objectives b) Is correct c) Is not correct. Because they are defensive in nature d) Is not correct. Because they define certain standards that help define practices – the standards should be responsive to changes in the threats	-	-	1
45	b	a) Is not correct. Because it is too late then b) Is correct. By defining the security standards, each party can then determine what is required and further specify those requirements c) Is not correct. Because the security agreements are likely to be kept private d) Is not correct. Because contracts do not usually change in this way	-	-	1