Sample Exam – Questions

Sample Exam set notation of exam paper

Version Final

ISTQB® Security Test Engineer Syllabus Specialist Level

Compatible with Syllabus version 1.0

International Software Testing Qualifications Board

Version Final

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 ISTQB®: names of participants

The core team thanks the Exam Working Group review team, the Syllabus Working Group and the National Boards for their suggestions and input.

Revision History

Sample Exam – Questions Layout Template used:	Version 2.6	Date: September 20, 2023

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:

- Questions[1], including for each question:
  - Any scenario needed by the question stem
  - Point value
- Response (answer) option set
- Additional questions, including for each question [does not apply to all sample exams]:
  - Any scenario needed by the question stem
  - Point value
- Response (answer) option set

- Answers, including justification are contained in a separate document

[1] In this sample exam the questions are sorted by the LO they target; this cannot be expected of a live exam.

Questions

Question 1 (1 Point)

Which one of the following BEST describes the security level of assets regarding integrity?

a) Authenticated users should be granted access to files and applications
b) Only file owners can be granted access to modify data to establish proper integrity
c) The record history must be kept for two years to fulfil the integrity objective
d) Establish a process that allows users to access unchanged data whenever they need it

Select ONE option.

Question 2 (1 Point)

Which one of the following is adequate alternative to describe how security testing can verify that confidentiality of sensitive information has proper safeguards?

a) Security testing verifies if there are proper access controls that prevent unauthorized access to confidential information
b) Security testing verifies if there are proper controls that prevent only authorized updates can be made and all data remains reliable
c) Security testing checks for quick recovery mechanisms to restore services promptly after an incident
d) Security testing ensures that the organization's response to incidents is effective, minimizing damage and downtime

Select ONE option.

Question 3 (1 Point)

Which of the following option BEST describes a security audit?

a) A high-level description of security testing and overall security strategy
b) A systematic evaluation of the security information system by measuring how well it conforms to an established set of criteria
c) Audit helps to stop unauthorized intruders from accessing the system
d) Audit helps to reduce costs by shutting down hardware and software that cause risks of vulnerability

Select ONE option.

Question 4 (1 Point)

Which one is the BEST alternative to describe Zero Trust?

a) There is not a single point of trust.
b) All devices and users are trusted by default.
c) It is a security model that inherently trusts everything inside the network.
d) A Zero Trust system ensures that everybody can access data if they have the proper credentials.

Select ONE option.

Question 5 (1 Point)

Which TWO of the following would you include to verify that the concept of Zero Trust has been correctly implemented?

a) Controls which check for every individual access request to each sensitive resource.
b) Access requests that are initiated by always trusted non-human service accounts.
c) Control if access logs produced by the system provides a permanent, time-stamped record information of all activities.
d) Control of organizational policies because they are not applied when defining Zero Trust security mechanism.
e) Focus on access controls to external network instead of controls to specific applications, resources, data, and assets.

Select TWO options.

Question 6 (1 Point)

If you use an open-source software, which ONE of the following is an important consideration for tool maintenance?

a) Reliability of the vendor and ability to provide support
b) Frequency and availability of updates from the vendor
c) Technical capabilities of your team to support and customize the tool for your environment
d) License cost and support contract cost

Select ONE option.

Question 7 (1 Point)

A bank has subcontracted the development of new features for its customers portal, to improve its user experience. The development of the features is finished and has been delivered to the bank.

The bank calls you to do plan and perform security tests on a pre-production environment before the deployment. What might be your proposal?

a) Execute white-box testing to cover all the source code and be sure that there are no more defects before the deployment.
b) Execute black-box vulnerability scanning to be sure that all known vulnerabilities in the scope of the project, potentially exploitable by an attacker, are or will be identified.
c) Execute black-box fault injection testing to find potential vulnerable entry points.
d) Verify that the security coding rules have been applied using a static application security testing tool.
e) Check whether vulnerabilities detected by white-box testing could be exploitable.

Select TWO options.

Question 8 (1 Point)

You are the security test engineer in a development team. You must define the security test techniques that must be applied as static security testing. What might be your proposal?

a) Check that security coding rules are applied by the developers then check that the security requirements are complete.
b) Check that the set of security requirements is pertinent and complete, check that the coding rules are applied by the developers, then build the application and execute some SQL injections to check that input fields are correctly protected against SQL injection.
c) Check that the security requirements are complete, then check that the design has followed “security by design” best practices then check that security coding rules are applied by the developers.
d) Execute boundary value testing on the built application to check that buffer overflows are avoided by applying dedicated security coding rules.

Select ONE option.

Question 9 (1 Point)

You have been given the following requirement for security testing:

A user will be allowed to request their password. If they make this request, they must answer two of their three security questions correctly. If they answer correctly, a link will be sent to their email. The link will take them to a page where they can reset their password. Once reset, they can login with the new password. The link must be disabled 1 hour after it is sent. The user is allowed only two password requests without a reset, after which they will have to call the help desk. For any other errors, the user ID is locked and must be unlocked by the help desk.

Which of the following is the minimum list of test conditions to adequately test the functional security covered by this requirement?

a) Invalid user; valid user; 2 correct answers; 2 incorrect answers; good email; bad email; reset with good password; reset with bad password; link good; link expired; two requests without reset; three requests without reset
b) Valid user; 2 correct answers; good email; reset with good password; link good; two requests without reset
c) Invalid user; 2 incorrect answers; bad email; reset with bad password; link expired; three requests without reset
d) Buffer overflow on each input field; SQL injection on each input field; cross site scripting (XXS) on the login page and reset password page, invalid user; valid user; 2 correct answers; 2 incorrect answers; reset with good password; reset with bad password; link good; link expired; two requests without reset; three requests without reset

Select ONE option.

Question 10 (1 Point)

In your organization, you are responsible for Identification & Access Management activity to manage and maintain users accounts and rights. During the last two months, there have been two new comers and one person from the company changed department. Their profile has been assigned to the roles and rights. According to your responsibility, what security test techniques must you plan?

a) No testing is necessary because accounts and rights have been managed.
b) Review roles permissions, after gathering all applied modifications.
c) Fuzz the role(s) of the newcomers to be sure that roles and privileges settings to these newcomers are correct.
d) No testing is necessary because the newcomers have basic roles and privileges and the person who changed department has less privileges than before.
e) Having applied the changes, check whether the access to new applications is working.

Select TWO options.

Question 11 (1 Point)

What are key attributes of security authentication of a medium complexity system?

a) It verifies that the user has the correct profile and corresponding rights to access limited parts of the system
b) It is key in identifying the amount of system resources the user can utilize

c) It verifies that user entering the system is legitimate
d) It uses common credentials among users to gain entry into the system

Select ONE option.

Question 12 (1 Point)

Typical encryption mechanisms are vulnerable to threats which makes it important to understand their effectiveness at any given time. Identify which of the following you should implement to gain confidence in your encryption mechanisms?

a) Evaluate cryptographic keys to ensure they are at minimum 768 bits in size
b) Ensure you are applying random algorithms to generate random numbers where possible
c) Develop tests that ensure the chosen symmetric encryption is used with the correct setup and parameters
d) Ensure that all the events are logged in log files with all the sensitive information available

Select ONE option.

Question 13 (1 Point)

You are implementing procedures for evaluating system hardening in an effort to test the system's security effectiveness. What procedure might you follow to ensure the hardening mechanisms put in place are working as expected?

a) Closely monitor various security performance reports and metrics to determine if the correct level of access and authentication is achieved
b) Frequently audit strong authentication to ensure a high level of intrusion protection is maintained at all times
c) Evaluate the hardware components that have been hardened and compare these to other hardened software components to ensure equilibrium is being achieved
d) Enlist a known hacker to conduct an independent assessment of the hardening effectiveness

Select ONE option.

Question 14 (1 Point)

You are responsible for all aspects of the security process, including testing. For this particular task you are to use high-level tests as a basis for manual tests and execute these from an external vendor's perspective. Which security test task can be done in parallel with this?

a) Security test creation of test conditions and test objectives
b) Security test implementation
c) Overall evaluating and reporting of security testing
d) Security test analysis and design

Select ONE option.

Question 15 (1 Point)

Which of the following are main characteristics of an effective security test environment?

a) Closely tied to production systems to enhance security at all points
b) Isolates different old versions of the operating systems for use in the environment
c) Mimics the production environment in terms of access rights
d) Includes all production environment plug-ins as well as other plug-ins not in the production environment to ensure the most comprehensive setup

Select ONE option.

Question 16 (1 Point)

During component testing, why should the security tester review compiler warnings?

a) Because these indicate security problems that must be fixed
b) Because these indicate potential issues that should be investigated
c) Because these indicate coding issues that will cause functional suitability defects
d) Because these indicate poor programming practices that will increase maintainability

Select ONE option.

Question 17 (1 Point)

You have been testing a system that has 20 defined components. You have done extensive security testing on each of the components. The system is now ready to move into component integration security testing. How should you approach this testing?

a) Since component integration testing is concerned with the summation of the vulnerabilities of the individual components, repeating the tests on the integrated components is the best approach.
b) The main risk is now in the integration of the components themselves, so testing should cover each interface and verify that there are no vulnerabilities in the interfaces and the components should also be retested.

c) It is likely that new vulnerabilities are present with the integrated components as well as with the larger system and infrastructure that is now testable, so testing should expand to include these new areas.
d) Since the components are now integrated, the security risks will be reduced because the possible interactions are now limited so only the integration points should be tested and no component confirmation testing is needed.

Select ONE option.

Question 18 (1 Point)

Which of the following test cases would best cover a system's security access procedure?

a) Three unsuccessful login attempts will generate a lock-out message. Contact your manager or the System Administrator so they can give you a temporary password over the phone. You must then change the temporary password upon logging in. You log out then log back in using your newly created password.
b) You receive a lock-out message after several attempts to log in. You call Information Technology (IT) support to obtain a new password. You log in with the temporary password, log back out, then log in again and enter a new password.
c) After several attempts you are locked out of the system. You use a password that worked previously. However, it no longer works. You attempt to create a new password, but you are now locked out. A complete reboot of the machine is the next step to take you to the prompt to re-enter the password.
d) After the first attempt to use an invalid password, you immediately pull up a list of passwords on your notepad on your PC to ensure you are using the correct one. You try another password from the list, and it works.

Select ONE option.

Question 19 (1 Point)

You are asked to perform security testing on a new application that should go live. There are no explicit requirements, so you select your own test cases from standards and best practices.

Which three (3) of the following statements guide you best for selecting test cases?

i. Norms are valid input as they are approved by a recognized body of knowledge
ii. Standards can be classified into industry standards, de facto standards and manufacturer specific standards. Industry standards and de –facto standards are valid input, manufacturer standards might not fit to a specific context
iii. As standards are mandatory, they are valid input as they must be applied in all environments

iv. Best Practices are no valid input as they are usually on very high level
v. De-facto-Standards are good input as they often have their roots in industry standards

a) i, ii, and v
b) i, ii, and iii
c) ii, iii, and v
d) iii, iv, and v

Choose ONE option.

Question 20 (1 Point)

A new start-up enterprise in the banking industry has developed a new core system. The development team has focused on good usability and excellent performance so far. Before going live, the executive board wants to get an independent view about the level of security. They are asking you as security tester to do a black-box-pentest. The task is to test for the most critical vulnerabilities that could be exploitable for the new banking app.

If you want to fulfill this job, how can you leverage standards for your task?

a) You select relevant weaknesses within CWEs standard and execute listed test cases.
b) You select relevant weaknesses within CWE, choose available exploits for selected CWEs and apply them
c) You select relevant weaknesses within CWE, you prioritize selected CWEs based on CWSS standard, and you select relevant CVEs covering prioritized CWE
d) You select relevant weaknesses within CWE, you prioritize selected CWEs based on CWSS standard and derivate individual test cases related the CWSS
e) For each selected CVE you derive test cases for the banking app and execute them

Choose TWO options

Question 21 (1 Point)

When you use test oracles for an application from standards and best practices, what do you have to consider?

a) Such test oracles are valid independent from any application parameters
b) Such test oracles can only be used as fuzzy hints for security testing
c) Such test oracles can not be used for security testing
d) The less specific an application and its context is, the more efficient is reusing such test

Choose ONE option.

Question 22 (1 Point)

Best practices and standards deliver many artefacts, which can be used effectively for security testing. Which combinations of artefact and activity maps correctly?

1. Consistent nomenclature
2. Expert knowledge
3. Benchmarking
4. Holistic security overview

which can be used for:

A. easier communication
B. reusing security expert knowledge for security testing
C. doublecheck completeness of security testing activities
D. easily demonstrate effectiveness of applied security testing activities

a) 1-A, 2-B, 3-D, 4-C
b) 1-A, 2-B, 3-C, 4-D
c) 1-D, 2-A, 3-B, 4-C
d) 1-B, 2-D, 3-A, 4-C

Choose ONE option.

Question 23 (1 Point)

You are hired as a security tester by the management of a medium-sized engineering company that produces different parts for automotive and is strongly dependent on their suppliers, as the price for raw materials does directly affect the profit. The company does only have a public web site and a well-known mail domain but does not offer further web services. Your task is to gain access to the internal production environment consisting of several modern industrial facilities and compromise at least one system.

Which TWO options present best how you could take advantage of the organizational context?

a) Infiltrate one of the most used suppliers to get closer to the actual target company
b) Perform a social engineering attack by faking to be an existing or a new potential supplier and try to learn more about the target, e.g. by visiting and asking for a short viewing
c) Identify the mail address of the accounting department and send fake billings containing malicious content e.g. for gaining remote access via a reverse shell
d) Scatter USB sticks around the companies' building and wait until someone collects a stick and plugs it in.
e) Do a brute force against the SSH login of the web server

Choose TWO options.

Question 24 (1 Point)

Your company develops different products for the aviation industry. At the beginning of the year, a new product was announced. For the first time, this will be a communication device. Your job is to perform security testing of the new product before it is launched on the market.

Which ONE of the following aspects describes BEST what you do have to consider?

a) Aviation Industry is a regulated sector; therefore, the new product and the complete development process must be compliant with current regulations.
b) Some countries have their own regulations regarding radio antennas and used standards. The product must work properly, even though some frequencies might interfere with the frequencies used by the product
c) The security tests need to be executed very fast, since the product must be launched as soon as possible
d) Employees need to prove their knowledge about radiocommunication through personal certifications

Choose ONE option.

Question 25 (2 Points)

During security testing a core system you find several suspicious files that were neither created by you or other testers during the testing nor used by the applications running on that system.

Choose the option BEST describing how you would proceed

a) Continue the security test and report your findings after you have finished all testing activities
b) Pause the security test and write an informative global e-mail at least to all colleagues who have access to the system. Continue, if no one has a plea.
c) Stop the security test and shutdown the system immediately, because there has been an unauthorized access and further potential harm must be prevented
d) Stop the security test and follow the steps defined by the companies ‘security policy for reporting an incident. If there is no policy for incident reporting, report to the person who is responsible (e.g., IT Security Officer, CISO…)
e) Stop the security test and start investigations and follow the steps defined by the companies’ security policy for investigation

Choose ONE option

Question 26 (2 Points)

Each attack is different. However, certain steps are common for almost every attack. These steps can be defined as:

a) Information gathering step, followed by exploitation/gaining access and at the end persisting/maintaining access.
b) Social engineering, followed by brute-force attack and at the end persisting/maintaining access
c) Exploitation/gaining access followed by social engineering to understand the results and at the end clearing tracks
d) Information gathering, followed by clearing tracks and at the end social engineering to have a better baselining.

Choose ONE option

Question 27 (1 Point)

Which ONE of the following statements describes BEST how security testing should be implemented in the development lifecycle?

a) Each development activity should have a corresponding security testing activity
b) With performing a proper threat analysis and security design most vulnerabilities can be found
c) SAST and DAST should be executed in all software development lifecycle phases
d) Security testing should be performed during all software development lifecycle phases to keep in sync with manual functional testing

Choose ONE option.

Question 28 (2 Points)

Which TWO of the following statements does BEST describe the impact of a software development model on security testing?

a) The team may involve a security enabling team to perform the security testing in every model
b) The waterfall model does best support security testing during its software development lifecycle
c) DevOps may give a better support for security testing to be performed during operations

d) It is easier to perform security testing using Kanban compared to using Scrum
e) Security testing can be better planned using the Agile software development models compared with the Waterfall model

Choose TWO options.

Question 29 (1 Point)

Which of the following four statements is true for security testing within the context of maintenance testing?

a) Focusing on confirming satisfaction of all security requirements after the change
b) Running the existing regression set against individual functions to check the change works
c) Testing for new vulnerabilities that might have been introduced by the change.
d) Running confirmation and regression security tests after a change is made

Choose ONE option.

Question 30 (1 Point)

Which of the following describes BEST why you should analyse security testing results?

a) To gain understanding of specific security threats and risks based on security assessments, audits and standard sources of known vulnerabilities
b) To translate conceptual tests into tests that can be executed either manually or with tools
c) To define an appropriate scope of testing that corresponds to the security risks.
d) To bring the security testing 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

Choose ONE option.

Question 31 (1 Point)

You are responsible for the system's security. Somebody in your team is interested in security testing and does a penetration test on your system, which includes OWASP Top-10 vulnerabilities. The corresponding test report consists only of succeeded and failed testcases covering these vulnerabilities. Which reasoning on accepting or rejecting the test report is correct?'

a) Accepting, as the penetration test was done by an internal colleague who knows the specific security style guides.
b) Rejecting, as your acceptance criteria for security were not communicated and are not considered in the test report. So it's unclear if the corresponding test techniques were used and if the test results are relevant for your yearly security style guide conformance check.
c) Accepting, as OWASP is Best Practice and defines a general list of acceptance criteria
d) Rejecting, because a security code style guide should be tested by white-box testing approaches, not by black-box dynamic pentests.
e) Accepting, as OWASP reflects your security code style guide.

Choose TWO options.

Question 32 (1 Point)

To leverage security testing to the highest level of efficiency and effectiveness it must:

a) Be integrated into an overall security process, that tries to minimize risk and ensure business continuity.
b) Be applied on a yearly basis for all used IT-systems
c) Be used to pro-actively limit the impact of a security breach
d) Consider d2y-to-day communicated vulnerabilities.
e) Be guaranteed, that all identified vulnerabilities are remediated within an appropriate timeframe smaller 6 months

Choose TWO options.

Question 33 (1 Point)

Typical dimensions that a security test engineer can use for enhancing ISMS scope are:

1) Adding additional test objects to his test scope
2) Adding additional test techniques to his test design
3) Improve test coverage while sticking on given test objects and test approaches
4) Increase automation of security test execution

Which can be used for:

A. bringing in additional insights into a given system that can be used to enhance an existing ISMS
B. identifying additional weaknesses for known components to enhance an existing ISMS
C. identifying additional weaknesses for components that are not yet part of the overall ISMS.
D. making the existing IT-system more secure.

Which one of the following alternatives presents the correct pairing of the security test engineer's actions and goals?

a) 1-C, 2-A, 3-B
b) 1-B, 2-D, 3-B
c) 1-C, 2-A, 4-B
d) 2-D, 2-C, 4-A

Choose ONE option.

Question 34 (1 Point)

How can security testing improve measurability within an ISMS?

a) Security tests can be used as objective analysis within the Check step of the PDCA cycle to measure effectiveness of a PDCA cycle.
b) All Security testing generates quantifiable insights into the security of a system that can be used to measure ISMS effectiveness.
c) The more security tests pass a test for a system under test, the better and more effective the ISMS is.
d) The effectiveness of an ISMS is better the more security testing techniques are used.

Choose ONE option

Question 35 (1 Point)

Security Test reports should be handled with a high level of confidentiality. What type of data being part of most security test reports motivates this classification?

a) Name of the security tester, timeframe for test execution, test results (passed and failed test cases)
b) Used test environment, pre-set preconditions of the executed tests, used test data, procedure of test execution, detected behavior
c) List of tested CVE vulnerabilities, list of named developers, identified software development method, identified software development tools
d) Used security coding conventions, identified functional test coverage, applied vulnerability scans

Choose ONE option.

Question 36 (1 Point)

Imagine you executed some security test cases as part of a penetration test for a business-critical system. One of it failed and it looks like you have identified a possible vulnerability, which might have some dramatic impact for the business. What to do before you directly motivate its mitigation?

a) Vulnerability demarcation, i.e. to execute similar test cases to identify demarcation of identified vulnerability.
b) Effort estimation for mitigation action, i.e. to do a break down structure of intended mitigation
c) Mitigation design, i.e. to design the solution mitigating identified vulnerability
d) Risk adjustment 1, i.e. to doublecheck that the identified vulnerability can be exploited on production
e) You immediately start to mitigate the identified vulnerability.

Choose TWO options.

Question 37 (1 Point)

Imagine you have identified a vulnerability on CVSS level 9.8. You have doublechecked that this vulnerability can even be exploited on production, and the business confirmed that this vulnerability can have very strong negative impact. On the other hand, the application is business critical, so it is decided to mitigate the identified risk associated with the identified vulnerability: What's your recommendation:

a) If the vulnerability affects a specific feature set it should be analyzed if it is possible to switch off the specific feature containing the vulnerability.
b) In most cases it's easier to block specific traffic on the network layer, so the task is to block the specific vulnerable traffic within the firewall.
c) If you have a modern web application firewall vulnerabilities are automatically identified and mitigated.
d) If you can add an additional security control to the list of users (e.g. by IP-filtering or adding MFA) it can be considered to reduce the risk probability by this technique.
e) In most cases the fastest and cheapest mitigation action is to avoid it completely by repairing the affected systems vulnerability.

Choose TWO options.

Question 38 (1 Point)

In a CI/CD environment a new pipeline is being put together for the next project you are working on. Which one of the following would you recommend being the first triggered step as part of the pipeline?

a) SCA
b) SAST
c) DAST
d) IAST

Choose ONE option.

Question 39 (1 Point)

Which of the following test scanners & methods are scanning the application under test during run time?

a) DAST
b) Static analysis
c) SCA
d) SAST

Choose ONE option

Question 40 (1 Point)

Which test objects can be scanned by static testing tools?

a) Configuration files
b) Security design
c) API endpoints
d) Processes in RAM

Choose ONE option.