Sample Exam – Questions

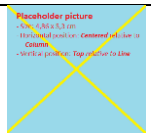
Sample Exam set notation of exam paper

Version 1.0

ISTQB® Security Test Analyst Syllabus Specialist Level

Compatible with Syllabus version 1.0

International Software Testing Qualifications Board



Version 1.0 30.10.2026

© International Software Testing Qualifications Board



Copyright Notice

Copyright Notice © International Software Testing Qualifications Board (hereinafter called ISTQB®).

ISTQB® is a registered trademark of the International Software Testing Qualifications Board.

All rights reserved.

The authors hereby transfer the copyright to the ISTQB®. The authors (as current copyright holders) and ISTQB® (as the future copyright holder) have agreed to the following conditions of use:

Extracts, for non-commercial use, from this document may be copied if the source is acknowledged.

Any Accredited Training Provider may use this sample exam in their training course if the authors and the ISTQB® are acknowledged as the source and copyright owners of the sample exam and provided that any advertisement of such a training course is done only after official Accreditation of the training materials has been received from an ISTQB®-recognized Member Board.

Any individual or group of individuals may use this sample exam in articles and books, if the authors and the ISTQB® are acknowledged as the source and copyright owners of the sample exam.

Any other use of this sample exam is prohibited without first obtaining the approval in writing of the ISTQB®.

Any ISTQB®-recognized Member Board may translate this sample exam provided they reproduce the abovementioned Copyright Notice in the translated version of the sample exam.

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 Member Boards for their suggestions and input.

The following participated in reviewing: Aneta Derkova, Jan Sabak, Klaus Skafte, Frank Neirynck, Gary Mogyorodi, Kamila Kozakovičová, Meile Posthuma, Piet de Roo, Ray Gillespie and members of the ISTQB examination work group.

© International Software Testing Qualifications Board



Revision History

Sample Exam – Questions Layout Template used:	Version 2.11	Date: October 16, 2023

Version	Date	Remarks
1.0	30.10.2026	Release version

© International Software Testing Qualifications Board



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
Questions....7
Question #1 (1 Point)....7
Question #2 (1 Point)....7
Question #3 (1 Point)....7
Question #4 (1 Point)....8
Question #5 (1 Point)....8
Question #6 (1 Point)....8
Question #7 (1 Point)....9
Question #8 (1 Point)....9
Question #9 (1 Point)....9
Question #10 (2 Points)....10
Question #11 (1 Point)....10
Question #12 (1 Point)....11
Question #13 (1 Point)....11
Question #14 (1 Point)....12
Question #15 (1 Point)....12
Question #16 (1 Point)....13
Question #17 (1 Point)....13
Question #18 (1 Point)....13
Question #19 (1 Point)....14
Question #20 (1 Point)....14
Question #21 (1 Point)....15
Question #22 (1 Point)....15
Question #23 (2 Points)....15
Question #24 (1 Point)....15
Question #25 (1 Point)....16
Question #26 (1 Point)....16
Question #27 (1 Point)....17
Question #28 (1 Point)....17
Question #29 (1 Point)....17
Question #30 (1 Point)....18
Question #31 (1 Point)....18
Question #32 (1 Point)....19
Question #33 (1 Point)....19
Question #34 (1 Point)....19
Question #35 (1 Point)....20
Question #36 (2 Points)....20
Question #37 (1 Point)....21
Question #38 (1 Point)....21
Question #39 (1 Point)....21
Question #40 (2 Points)....22
Appendix: Additional Questions....23

© International Software Testing Qualifications Board



© International Software Testing Qualifications Board



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.

© International Software Testing Qualifications Board



Questions

Question #1 (1 Point)

A Security Test Analyst is participating in a risk assessment workshop for a digital banking platform. The security test analyst is asked to explain the concept of an “asset” in the context of security testing for banking platforms.

Which of the following statements BEST explains what an asset is in this context?

a) An asset is any digital element within the organization that can potentially be affected by a security vulnerability, and can be associated with a specific threat scenario during risk evaluation.
b) An asset is any technical component within the system architecture that stores or processes data, including hardware and software elements, and it directly participates in system functionality and operational workflows.
c) An asset is any resource that is documented in the system design or architecture diagrams and is assigned ownership and classification as part of compliance processes within the organization.
d) An asset is any item, that contributes to information processing or business operations and has value to the organization, thereby requiring appropriate protection against potential security threats and risks.

Select ONE option.

Question #2 (1 Point)

Which factor is typically excluded from the estimation of an IT asset’s value in security risk management?

a) The time and effort required to recreate or reobtain the asset - this expense is included in the valuation because it reflects direct costs and business interruptions.
b) The potential damage caused by the asset’s loss - such effects are included in the valuation, as they determine the economic and operational value of the asset.
c) The associated threats and vulnerabilities, that enable prioritization according to potential exploitation scenarios that subsequently help derive economic impact of compromise.
d) Legal liabilities arising from data breaches - legal and regulatory consequences are included in the valuation, as they can have significant financial and operational implications.

Select ONE option.

Question #3 (1 Point)

In preparation for a penetration testing engagement, a Security Test Analyst must identify security risks that are both critical to asset protection and practically testable using technical security test techniques. The identified assets include sensitive data, encryption systems, and operational infrastructure.

Which TWO risks should be selected as the highest priority for testing the production environment?

a) The existence of unpatched vulnerabilities in systems due to ineffective patch management processes, allowing attackers to exploit publicly known weaknesses across applications, servers, and connected infrastructure components.

© International Software Testing Qualifications Board



b) Inadequate security policies for the secure disposal of physical storage devices, which may result in data exposure by persons likely to get hold of decommissioned systems and try to clean data from that hardware.
c) Deficiencies in cryptographic key management, including insecure data transfer and data storage and absence of proper password rotation mechanisms, which undermine the confidentiality and integrity of protected data assets within the system.
d) Insufficient security incident response planning, which can delay recovery efforts and increase damage during security incidents and would give hackers ample time to navigate in the system before they are detected.
e) Weak environmental controls in critical high-security facilities, including lack of fire suppression and unstable power supply systems, which primarily impact availability through operational failures rather than targeted attacks.

Select TWO options.

Question #4 (1 Point)

During a risk assessment for organizational assets, which factor is most critical when evaluating the risk likelihood that a threat will successfully exploit a vulnerability?

a) The cost to replace the asset if compromised.
b) The ease with which an attack can be executed.
c) The number of assets identified in the inventory.
d) The organization’s risk appetite statement.

Select ONE option.

Question #5 (1 Point)

A Security Test Analyst evaluates attacker profiles including financially motivated attackers, hacktivists, and insiders seeking revenge. The analyst wants to use this knowledge to refine the test approach and improve risk-based prioritization.

Which of the following BEST illustrates how knowledge of attacker motivations enhances the analyst’s effectiveness?

a) It enables the analyst to anticipate likely attack strategies and prioritize testing of scenarios aligned with attacker goals, such as data theft for financial attackers or service disruption for politically motivated actors.
b) It enables the analyst to complete threat modelling by incorporating attacker motivations into the identification of potential attack scenarios, confirming that testing reflects both security vulnerabilities and realistic threat behaviors.
c) It enables the analyst to enhance risk assessment by linking attacker motivations with asset exposure, confirming that assets are evaluated against a broader range of possible threat conditions and attacker intentions.
d) It enables the analyst to strengthen testing completeness by confirming that different attacker motivations are systematically considered during test planning, thereby improving coverage across multiple threat categories.

Select ONE option.

Question #6 (1 Point)

Which TWO of the following test activities BEST simulate attacker reconnaissance using passive information gathering methods?

© International Software Testing Qualifications Board



a) Searching employee profiles on social media to identify roles and technologies used within the company.
b) Performing external network scanning to identify open ports and exposed services, thereby mapping the attack surface through controlled review of internet-facing systems.
c) Reviewing job postings and recruitment materials to identify information about internal tools, frameworks, and infrastructure components based on advertised technical requirements.
d) Sending carefully crafted phishing emails to selected employees to observe responses and collect authentication data for further analysis of system access controls.
e) Conducting DNS enumeration and querying publicly accessible domain registration records to identify subdomains, infrastructure providers, and related organizational assets without direct system interaction.

Select TWO options.

Question #7 (1 Point)

Which ONE of the following scenarios BEST represents an insider risk that combines both technical and social factors?

a) An employee unintentionally installs malware after clicking on a phishing link that came via a high-priority email, allowing external attackers to gain access to internal systems through compromised credentials.
b) An external attacker impersonates an employee by spoofing email addresses and attempts to trick staff into revealing confidential information without having legitimate access to internal systems.
c) An employee sends emails from their trusted internal account requesting sensitive information from colleagues, leveraging their legitimate system access.
d) A system administrator performs routine updates but accidentally introduces configuration errors that temporarily weaken system security without exploiting their access for malicious purposes.

Select ONE option.

Question #8 (1 Point)

Which ONE of the following alternatives best distinguishes between external attacker and insider in the context of security testing?

a) An external attacker focuses on misusing privileges, while an insider does not consider any context.
b) An external attacker focuses on exploiting system vulnerabilities, while an insider can bypass many of those barriers by abusing legitimate credentials to reach restricted areas.
c) An external attacker targets weaknesses accessible to individuals with authorized access, while an insider attempts to bypass perimeter defenses.
d) An external attacker evaluates how defenses can be exploited, while an insider identifies vulnerabilities in public-facing assets.

Select ONE option.

Question #9 (1 Point)

Risk analysis is often done while taking into consideration the specific context. This is because the context might influence the risk likelihood and risk impact of any security vulnerability.

© International Software Testing Qualifications Board



Which TWO parameters among the below listed options would typically have the most important risk impact on the context for which risk analysis has to take place?

a) Typical objectives of the organization, their core activities and specific regulations that are valid.
b) The financial Budget that is available for risk management
c) Risk management tool, that is used for professional risk management
d) Methods, programming languages and databases that are used
e) External supplier and their dependencies on core activities

Select TWO options.

Question #10 (2 Points)

You work as security test analyst for a regulated bank. A preliminary security test reveals multiple severe vulnerabilities in early development, each having its own CVE and CVSS value. Some of the identified vulnerabilities have a CVSS base score greater than 9, indicating a high-risk level.

As the security test analyst, what would you advise management to do next?

a) Risk acceptance: As the security test was done early in the software development lifecycle the identified risks do not really show strong risk impact.
b) Risk delegation: As the security test was done early in the software development lifecycle the risk is more on developer side as on company side. They are responsible for fixing the defects.
c) Risk mitigation: Identified risks have to be mitigated as soon as possible to apply shift left. The earlier the mitigation is done in the software development lifecycle, the more efficient the correction might be.
d) Risk avoidance: As the severity of the identified security failures is high, your advice is to exclude the corresponding module from further development.

Select ONE option.

Question #11 (1 Point)

As security test analyst in an automotive company, your task is to test the consistency between given policies and the surrounding internal control system. Which of the following statements are valid to guide your activities when doing a security audit?

a) A policy is a set of ideas or a plan of what to do in particular situations. The internal control system's goal is to ensure compliance, and it consists of all policies to reduce overall risk. So, it's the task of the security test analyst to test the fulfilment of policies and to test if the internal control system identifies policy violations.
b) The policy of an organization is defined as the set of regulative requirements that must be fulfilled within an organization. An internal control system consists of all goal sheets for bonus salaries that are directly reflected by at least one policy. So, it's the task of the security test analyst to test all regulative requirements to generate necessary input for bonus salary definitions.
c) A policy is a set of ideas or a plan of what to do in particular situations. The internal control system is defined by the regulative context and is the master template for all policies refined on the next level. So, it's the task of the security test analyst to test the compliance between defined policies and the master template.
d) A policy describes the best practice for a specific discipline and how it is implemented in a given context. The internal control systems goal is to ensure compliance, and it consists of all policies to reduce overall risk. So, it's the task of the security test analyst to test if all best practices are implemented.

© International Software Testing Qualifications Board



Select ONE option.

Question #12 (1 Point)

You are working in a regulated industry. Your task is to support the effectiveness of policies as well as to improve their coverage in the internal control system.

Which of the below statements BEST indicates the MOST appropriate approach to start with in confirming the effectiveness of policies?

a) The internal control system defines the policies that a security test analyst must follow while executing security tests. So, you start by handing over the policies to the security test engineer.
b) Since the security test analyst is responsible for the internal control system you start to improve its quality by adding further security test touch points.
c) The internal control system is the master plan of all security test activities. So, your first task will be to extract the test execution plan for the security test engineer.
d) You start by defining corresponding test approaches for all security policies. Most of these security test activities should be related to the control system to underpin the relation to the policies.

Select ONE option.

Question #13 (1 Point)

A banking organization subject to regulatory oversight implements an Identity and Access Management (IAM) system. The applicable regulation explicitly requires that:

- Every access right must be approved and stored in a tamper-proof repository
- A reconciliation test must be conducted every 6–12 months
- All users with active permissions must still be employed by the organization

The Security Test Analyst is tasked with deriving test activities directly from these regulatory requirements within the Internal Control System.

Which of the following approaches BEST demonstrates correct application of deriving test activities from these regulations?

a) Systematically extract each regulatory control requirement and translate it into corresponding security test activities, including verification of approval traceability, perform reconciliation tests, and validation of employee status, confirming that each test case has clearly defined expected results directly mapped to the regulation.
b) Derive a comprehensive set of regulation-aligned test activities by interpreting the intent of access control requirements and extending them into additional validation scenarios, including approval consistency tests, reconciliation simulations, and employee lifecycle verification across multiple system states.
c) Define regulation-based test activities that focus on validating the effectiveness of access control enforcement mechanisms, including approval workflows, periodic review processes, and user-account associations, confirming that observed system behavior aligns with the overarching objectives of the regulation.
d) Develop a structured suite of test activities derived from regulatory principles that emphasize validation of access governance processes, including approval authorization, periodic access reviews, and user eligibility tests, while confirming consistency with broader compliance and audit expectations.

© International Software Testing Qualifications Board



Select ONE option.

Question #14 (1 Point)

Which of the following statements BEST explains the difference between security test objectives and security test strategy?

a) Security test objectives define the specific security testing aims to achieve, while the security test strategy describes the manner, scope, test techniques, and resources used to meet those objectives.
b) Security test objectives describe which test tools and test techniques should be used, while the security test strategy defines the compliance and assurance goals to be achieved.
c) Security test objectives are general guidelines, while the security test strategy focuses only on compliance with laws and regulations.
d) Security test objectives define what security test activities should be performed and when they should occur (for example, deciding the timing of penetration testing and security vulnerability scanning), while the security test strategy describes how these test activities are performed in practice across the test process.

Select ONE option.

Question #15 (1 Point)

A multinational insurance company is building a new cloud-based claims management system. The project is large, distributed across three countries, and follows a hybrid model: sequential planning for core components, agile sprints for customer-facing features.

Security is critical because:

- The system stores sensitive customer and financial data.
- It must comply with GDPR and PCI DSS.
- External regulators require evidence of a structured risk-based security testing process.

The initial test strategy was defined around functional requirements and performance testing, with no dedicated focus on security. After a regulatory review, management requests a comprehensive security test approach that:

1. Demonstrates compliance with external standards.
2. Identifies vulnerabilities early in the Agile software development.
3. Provides evidence of traceability from requirements to test execution.
4. Supports continuous integration/continuous delivery (CI/CD).

As the Security Test Analyst, you must recommend a suitable test strategy.

Which ONE of the below mentioned options represents the MOST suitable test strategy that may be adopted?

a) Adopt an Analytical Test Strategy with requirements-based test design, confirming that all security requirements are covered and traced.
b) Apply a Process-compliant Test Strategy, complemented by Regression-averse elements in the CI/CD pipeline.
c) Use a Model-based Test Strategy with threat modelling for test case design, applying attack vectors iteratively across sprints.

© International Software Testing Qualifications Board



d) Implement a Reactive Test Strategy with periodic penetration testing and security vulnerability scanning to capture high-priority risks.

Select ONE option.

Question #16 (1 Point)

An insurance company develops a web-based claims processing system using a hybrid SDLC approach that combines agile feature development with formal release management. During a sprint, a security test analyst notices that several third-party libraries have been added to the application and new APIs have been integrated into the backend services. Management requires early identification of vulnerable components and implementation weaknesses before the application enters system testing.

Which security test activity is MOST appropriate in this situation?

a) Software Composition Analysis (SCA) and Static Application Security Testing (SAST):
Analyze source code and third-party components during implementation to identify vulnerable libraries and insecure coding weaknesses.
b) Penetration testing:
Simulate attacks against the fully integrated production-like environment before release approval
c) Operational security monitoring:
Continuously monitor logs and production events to detect security failures after deployment.
d) Threat modeling:
Identify architectural threats, trust boundaries, and misuse cases during system design activities before implementation begins.

Select ONE option.

Question #17 (1 Point)

Match the characteristics of software testing work packages with their appropriate explanation from the list below:

1 Resources
2 Scope
3 Dependency
4 Metric

A. Measures to track progress of executing a WP
B. Financial expenses required to undertake a WP
C. Reliance on one WP with other tasks or WPs
D. Explicit definition of what is included and excluded in the WP

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

Select ONE option.

Question #18 (1 Point)

© International Software Testing Qualifications Board



A software company is developing a new financial application that handles sensitive customer payment data and must comply with PCI DSS regulations. Due to strict project deadlines, the project manager is concerned about the "unpredictable" nature of security testing.

Based on the provided text, which of the following actions BEST applies the specific characteristics and approach for defining a security test work package in this scenario?

a) Rely solely on a general requirement stating the system must be secured against the OWASP Top 10 to simplify the scope and meet the deadline.
b) Prioritize and time-box the exploratory manual testing efforts to maintain control over the unpredictable schedule while focusing on the most critical assets.
c) Assign the configuration and execution of security vulnerability scanning tools to the general functional test team to save on the cost of specialized competencies.
d) Perform all security testing at the very end of the implementation phase to determine the system is fully integrated before any security vulnerabilities are identified.

Select ONE option.

Question #19 (1 Point)

When a Security Test Analyst is planning the schedule and estimating the effort for security testing, which of the following BEST describes the activities they must consider?

a) Identifying if the budget and funding are sufficient for the entire project lifecycle.
b) Determining which security-related items must be implemented and tested before other testing occurs and estimating the time for regression tests.
c) Deciding whether the organization is comfortable with outsourcing the security tests to external vendors.
d) Defining the platform, technology, and physical location of the security test environment.

Select ONE option.

Question #20 (1 Point)

As Chief Security Information Officer (CISO) for a national bank, you are creating a security test plan to be compliant with the local cybersecurity framework. After analysis, you found that 11 systems/applications are within scope for extensive security testing. Some of the systems are procured and maintained by suppliers, others are developed and maintained in-house.

Which of the following options describes BEST your approach for creating this security test plan based on security testing work packages?

a) Perform risk assessments, discuss with the suppliers and developers who will perform what security testing, plan your security testing based on the given constraints.
b) Perform risk assessments, create security testing work packages for each system, assign those to the resources.
c) Carefully time box the use of the tooling based on a risk assessment. Specify the security testing scope and create security work packages based on the tooling needed, create the test plan.
d) Perform risk assessments, create an overview which system needs which security testing, create work packages and the test plan.

© International Software Testing Qualifications Board



Select ONE option.

Question #21 (1 Point)

Which of the following options represent the two MOST important key aspects for consideration in a test report?

a) Format of test report and used budget for security testing
b) Frequency of test execution and Audience of test report
c) Audience of test report, communication channel
d) List of used security test tools, certificates of security test engineer
e) Level of detail and confidentiality of listed information

Select TWO options.

Question #22 (1 Point)

Which among the options listed are the two MOST important tasks that a security test analyst should undertake in order to manage security test reports follow-ups for vulnerability mitigation?

a) Explanation of very technical aspects to non-IT-stakeholders.
b) Suggestion for and consulting for possible mitigation actions.
c) Implementation of mitigation actions.
d) Support of severity classification.
e) Organization of a task force of skilled developers to mitigate security incidents.

Select TWO options.

Question #23 (2 Points)

You are working in a highly regulated bank. You have received a security test report from the security test engineer who tested an application that should go live in a few days. The test report contains 5 high severity vulnerabilities. What are the TWO immediate next actions that should be taken from among the options listed below?

a) The STA should meet together with the STE and a developer to immediately fix directly the most severe security vulnerabilities.
b) The STA should create a high-level test report for management level to rethink the go-live. This test-report does not list any details but focusses on possible risks.
c) The STA should meet together with STE and developer to identify possible mitigation actions and the corresponding necessary efforts. The STE sends this list to the upper management and explains the different possible mitigation actions.
d) The STA creates a decision template for higher management to accept the risks of going live.
e) The STA forwards the initial test report to the upper management and asks for guidance on how to proceed.

Select TWO options.

Question #24 (1 Point)

© International Software Testing Qualifications Board



A Security Test Analyst wants to simulate how attackers perform active reconnaissance to map the attack surface before launching targeted attacks.

Which of the following actions BEST represents attacker-style active reconnaissance for this purpose?

a) Performing iterative port scanning and protocol reviewing against externally accessible systems to identify reachable services and potential entry points across the organization's network perimeter.
b) Sending targeted phishing emails to a subset of employees to determine whether employee system access credentials can be harvested and reused for accessing internal systems in the organization.
c) Gathering domain registration details, Domain Name Service DNS records, and publicly available infrastructure information to identify subdomains and hosting providers associated with the organization
d) Analyzing publicly disclosed vulnerabilities in commonly used software components to identify weaknesses that may be present within the systems environment of the organization

Select ONE option.

Question #25 (1 Point)

A company is preparing a major release of a cloud-based payment system. Due to regulatory requirements and increased threat exposure, management states that the security testing must demonstrate compliance with financial regulations, provide evidence that the system can withstand realistic attacks, and reduce high-risk level vulnerabilities before release.

To support this, the security team defines the test scope, selects penetration testing and security vulnerability scanning, decides on coverage and test tools, and assigns external security specialists.

Which of the following statements BEST differentiates security test objectives from security test strategy in this context?

a) Security test objectives define the intended security results while the security test strategy defines the way to achieve these results.
b) Security test objectives focus on selecting appropriate security test types, while the security test strategy is responsible for proving compliance and system resilience against attacks.
c) Security test objectives define high-level security goals, whereas security test strategy translates these goals into individual test cases and detailed test scripts.
d) Security test objectives and security test strategy differ mainly in timing, since objectives are defined after testing, and strategy is defined before testing begins.

Select ONE option.

Question #26 (1 Point)

A cloud service provider is rolling out a new file sharing platform for enterprise customers. The system will store confidential business data, and management is concerned about potential threats such as unauthorized access, data leakage, and privilege escalation. The security test team decides to derive test conditions directly from the security requirements and risk analysis to prioritize testing based on the most critical risks.

Which test strategy is the MOST appropriate for this situation?

© International Software Testing Qualifications Board



a) Analytical strategy:
Use risk-based analysis to derive security test conditions from requirements and prioritize tests by criticality.
b) Methodical strategy:
Apply a checklist from OWASP Testing Guide to cover common vulnerabilities.
c) Regression-averse strategy:
Perform security vulnerability scans after each build in the CI/CD pipeline.
d) Consultative strategy:
Ask enterprise customers which risks they think are most relevant for testing.

Select ONE option.

Question #27 (1 Point)

A healthcare software provider develops a cloud-based patient management platform using an agile DevSecOps approach. During a sprint review, the security test analyst identifies that a newly implemented feature processes sensitive patient information through several external APIs. The development team wants to identify potential attack vectors, analyze trust boundaries, and define misuse cases before the feature is integrated into the next release.

Which security test activity should the security test analyst apply FIRST in this situation?

a) **Continuous security monitoring**
Implement log analysis and automated security vulnerability scanning in production to identify operational security incidents after deployment.
b) **Threat modeling and security design review**
Analyze data flows, trust boundaries, attack vectors, and architectural weaknesses before implementation is finalized.
c) **Penetration testing**
Conduct simulated attacks against the fully integrated application before production release to evaluate exploitable vulnerabilities.
d) **Dynamic Application Security Testing (DAST)**
Execute runtime security tests against the deployed application during system testing to identify security weaknesses.

Select ONE option.

Question #28 (1 Point)

You are preparing the security test planning for a new complex application operated and managed in the cloud. You intend to use security test work packages to have better control and be able to adjust the workload more dynamically. The idea is to create a table mapping the different test objects to the possible security test types. Having created this table, how would you proceed to specify the different security test work packages?

a) Combine all identical test types in work packages
b) Define a work package for each test object
c) Perform a risk assessment for each test object
d) Prioritize the sequence of work package execution

Select ONE option

Question #29 (1 Point)

© International Software Testing Qualifications Board



You are creating a security test plan based on your identified and specified security test work packages. Your organization has a generic test plan template and you want to use this as a basis to create yours. What is the most likely part from the template to be reused in your security test plan and why?

Choose the BEST option

a) Context of the testing because it is important to identify and specify what will be tested in the prevailing context
b) Risk register because it will create a complete overview for the entire system risk position
c) Test strategy as it will describe all necessary details for the security testing that must take place
d) Schedule as this will show which work package shall be executed based on different parameters

Select ONE option.

Question #30 (1 Point)

A financial services organization conducts a security-focused Business Impact Analysis (BIA) on its online banking platform. The following protected assets and dependencies are identified:

- Customer Personally Identifiable Information (PII) stored in databases
- Web application servers handling authentication
- Backup storage systems hosted in a third-party cloud
- Internal employee access portals

The Security Test Analyst is evaluating potential risks affecting these assets and their dependencies.

Which of the following represents the MOST critical security risk scenario to prioritize?

a) A misconfiguration in encryption key management for customer PII could result in improper key rotation practices, potentially weakening data protection controls while still maintaining nominal encryption coverage across storage and transmission layers
b) Unauthorized access to the internal employee portal could enable privilege escalation, which may subsequently allow attackers to indirectly retrieve customer PII from backend systems through trusted service interactions
c) A failure in synchronization between primary and cloud-based backup systems could result in inconsistent data states, potentially leading to partial exposure of outdated customer records during restoration processes under certain operational conditions
d) Increased logging and monitoring across authentication services could introduce performance bottlenecks, which might indirectly affect system responsiveness during peak transaction periods while still preserving audit traceability

Select ONE option.

Question #31 (1 Point)

To maintain the integrity of an Information Security Management System (ISMS), an asset inventory must reflect the current state of the organization. Apart from periodic audits, which of the following scenarios represents a lifecycle event that triggers an immediate requirement to update the asset inventory?

© International Software Testing Qualifications Board



a) When the organization's annual security awareness training is completed
b) When the IT department schedules a routine security vulnerability scan
c) When an asset changes ownership, location, or is decommissioned
d) When the Chief Information Security Officer (CISO) reviews the quarterly budget

Select ONE option.

Question #32 (1 Point)

Which of the following scenarios BEST illustrates an insider threat caused by a careless employee or accidental insider, rather than a malicious or disgruntled insider?

a) An employee purposely copies a database of client contacts to a USB drive to take to a competitor for financial gain.
b) An HR manager ignores data privacy policies and intentionally browses colleague salaries out of personal curiosity.
c) A diligent staff member unwittingly clicks a link in a sophisticated phishing email, allowing malware to bypass the perimeter.
d) A third-party vendor deliberately modifies their access privileges to explore restricted areas of the network without authorization.

Select ONE option.

Question #33 (1 Point)

A regulation applicable to an organization requires that all external-facing applications must be penetration tested annually and that all critical vulnerabilities must be remediated within 90 days. The regulation does not define specific control activities.

The Security Test Analyst must derive appropriate test activities from these requirements.

Which of the following approaches BEST demonstrates correct derivation of test activities?

a) Establish a set of regulation-driven test activities that evaluate whether penetration testing practices and vulnerability remediation processes are consistently applied across all relevant systems, confirming alignment with regulatory timelines and security objectives.
b) Derive test activities that validate the organization's compliance with penetration testing and remediation expectations by assessing the completeness, frequency, and results of security assessments in relation to externally facing systems and identified vulnerabilities.
c) Define explicit test cases that verify the existence of recent penetration test reports for all external-facing applications and validate that all identified critical vulnerabilities have been remediated (or at least treated systematically) within the specified timeframe, confirming that each expected result directly reflects the regulatory requirement.
d) Create test activities based on regulatory expectations that assess both the execution of penetration testing and the effectiveness of vulnerability management processes, confirming that critical findings are identified, tracked, and resolved in accordance with compliance requirements.

Select ONE option.

Question #34 (1 Point)

© International Software Testing Qualifications Board



A security manager is preparing for a vulnerability assessment. He creates a document listing the specific IP addresses and web applications that the external testers are authorized to scan. He also explicitly lists two legacy servers that are **excluded** from the test to prevent accidental crashes.

Which aspect of security test planning is the manager primarily defining?

a) Scope Definition
b) Risk Assessment
c) Rules of Engagement
d) Reporting Requirements

Select ONE option.

Question #35 (1 Point)

A penetration tester delivers a final test report to the organization's Board of Directors. The test report is technically accurate but consists entirely of raw HTTP requests, lines of code, and complex vulnerability metrics. The Board rejects the test report, stating they cannot use it to make investment decisions.

Which key aspect of test report communication did the tester fail to apply?

a) Proof of Concept: The tester failed to prove that the vulnerabilities were actually exploitable.
b) Audience Suitability: The tester failed to provide a high-level executive summary linking technical risks to business impact.
c) Technical Veracity: The tester failed to include enough data for the IT team to reproduce the findings.
d) Methodology Declaration: The tester failed to explain which test tools and standards were used during the assessment.

Select ONE option.

Question #36 (2 Points)

A Security Test Analyst has completed risk identification and analysis, including risk likelihood and technical risk impact assessments. However, business impact and prioritization have not yet been formally incorporated. The analyst must determine the most appropriate next steps within a structured risk management methodology.

Which TWO actions BEST align with the correct progression of the methodology?

a) Engaging relevant business stakeholders to incorporate business impact considerations and refine risk evaluation, confirming alignment between technical findings and organizational priorities.
b) Preparing risk documentation that combines technical analysis with contextual information, enabling stakeholders to understand dependencies, potential consequences, and trade-offs during evaluation discussions.
c) Revisiting selected high-risk level scenarios to further refine exploitability assumptions, confirming that risk likelihood estimates are 100% robust before presenting results for evaluation.
d) Developing preliminary mitigation recommendations based on current analysis results, confirming that potential treatment options are available to support efficient decision-making.
e) Reassessing the scope of testing to include adjacent systems that may introduce additional dependencies, confirming that the overall risk landscape is as complete as possible prior to evaluation.

© International Software Testing Qualifications Board



Select TWO options.

Question #37 (1 Point)

An organization operates a large-scale Internal Control System (ICS) with numerous security policies and associated controls. The Security Test Analyst must determine that the ICS effectively enforces these policies.

Which of the following approaches BEST reflects correct application of the relationship between policies and internal control systems?

a) Confirming that each security policy is translated into clearly defined, testable control activities that can detect deviations and provide measurable feedback on compliance within the ICS.
b) Structuring control activities to align with organizational risk priorities while maintaining traceability between policies, implemented controls, and observed compliance results across systems.
c) Continuously reviewing and refining control implementations to determine they remain aligned with policy objectives as systems evolve and new risks emerge within the operational environment.
d) Coordinating control execution across teams to determine consistent enforcement of policies while optimizing resource utilization and minimizing duplication of effort within the ICS framework.

Select ONE option.

Question #38 (1 Point)

An organization relies heavily on automated security control activities within its Internal Control System, confirming consistent test execution with fixed test data, test tools, and environments. Over time, system updates introduce subtle behavioral changes that are not detected by the automated tests.

The Security Test Analyst suspects that the alignment between the system under test, the security test policy, and the automated test procedures may have degraded.

Which of the following actions BEST demonstrates correct application of security control activities?

a) Perform targeted spot tests to verify alignment between the security test policy, system behavior, and automated test procedures, and initiate necessary updates to the test policy, system, or test activities where discrepancies are identified to maintain the effectiveness of the control system.
b) Expand the automated test suite by incorporating additional regression scenarios derived from recent system changes, confirming that newly introduced behaviors are progressively covered while maintaining the existing structure of control activities.
c) Increase the frequency of automated security test execution and introduce parallel test runs across multiple environments to improve the likelihood of detecting subtle inconsistencies introduced by system updates
d) Strengthen configuration and change management processes to ensure that all system updates are thoroughly reviewed against existing security test cases prior to deployment.

Select ONE option

Question #39 (1 Point)

A Security Test Analyst is explaining how a risk management methodology aligned with ISO 31000 should be applied within a project.

Which of the following statements BEST reflects this methodology?

© International Software Testing Qualifications Board



a) Risk management is a structured process that establishes organizational context, conducts risk assessment and evaluation, applies treatment decisions based on business priorities, and integrates communication and monitoring activities to support continuous alignment with organizational objectives.
b) Risk management is a structured process that establishes organizational context, performs detailed risk assessment, prioritizes risks using standardized scales, and focuses on selecting optimal mitigation strategies supported by periodic stakeholder communication and review.
c) Risk management is a structured process that establishes organizational context, identifies and evaluates risks, applies treatment strategies such as mitigation and delegation, and supports these activities through stakeholder engagement and periodic process evaluation.
d) Risk management is a structured process that establishes organizational context, performs risk assessment, applies appropriate treatment strategies, supports stakeholder communication, and includes ongoing monitoring and improvement activities

Select ONE option.

Question #40 (2 Points)

You are reviewing a security test report for a web application. The test report lists the following vulnerabilities that are already adjusted to the specific context:

- SQL Injection in the login form (CVSS score: 9.8)
- Outdated TLS version (CVSS score: 6.5)
- Missing security headers (CVSS score: 4.3)

Which action among those listed below should be prioritized first, based on the severity described above?

a) Update the TLS version to the latest standard.
b) Add missing security headers to improve browser protection.
c) Fix the SQL Injection security vulnerability immediately.
d) Document all findings and schedule fixes for next quarter.

Select ONE option.

© International Software Testing Qualifications Board



Appendix: Additional Questions

NONE

© International Software Testing Qualifications Board