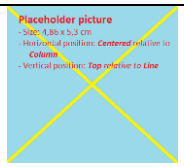
Sample Exam – Answers

Sample Exam set A
Version 1.0

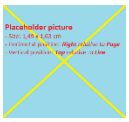
ISTQB® Security Test Analyst Syllabus Specialist Level

Compatible with Syllabus version 1.0

International Software Testing Qualifications Board



© 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.

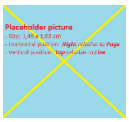
Acknowledgements

This document was produced by a core team from the 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 – Answers Layout Template used:	Version 2.11	Date: October 16, 2023

Version	Date	Remarks
V 1.0	30.10. 2026	Release version

© International Software Testing Qualifications Board

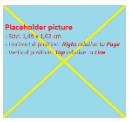
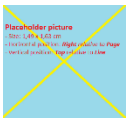


Table of Contents

Copyright Notice....2
Document Responsibility....2
Acknowledgements....2
Revision History....3
Table of Contents....4
Introduction....5
Purpose of this document....5
Instructions....5
Answer Key....6
Answers....7

© 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:

- Answer Key table, including for each correct answer:
  - K-level, Learning Objective, and Point value
- Answer sets, including 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*

© International Software Testing Qualifications Board



Answer Key

Question Number (#)	Correct Answer	LO	K-Level	Points
1	d	STA 1.1.1	K2	1
2	c	STA 1.1.2	K2	1
3	a, c	STA 1.1.3	K3	1
4	b	STA 1.2.1	K2	1
5	a	STA 2.1.1	K2	1
6	a, c	STA 2.1.2	K3	1
7	c	STA 2.2.1	K2	1
8	b	STA 2.2.2	K2	1
9	a, e	STA 3.1.1	K2	1
10	c	STA 3.1.2	K4	2
11	c	STA 3.2.1	K3	1
12	d	STA 3.2.2	K3	1
13	a	STA 3.3.1	K3	1
14	a	STA 4.1.1	K2	1
15	b	STA 4.1.2	K3	1
16	b	STA 4.2.1	K3	1
17	d	STA 5.1.1	K2	1
18	b	STA 5.1.2	K3	1
19	b	STA 5.2.1	K2	1
20	d	STA 5.2.2.	K3	1

Question Number (#)	Correct Answer	LO	K-Level	Points
21	c, e	STA 6.1.1	K2	1
22	a, d	STA 6.1.2	K2	1
23	b, d	STA 6.2.1	K4	2
24	a	STA 2.1.2	K3	1
25	a	STA 4.1.1	K2	1
26	a	STA 4.1.2	K3	1
27	c	STA 4.2.1	K3	1
28	a	STA 5.1.2	K3	1
29	d	STA 5.2.2	K3	1
30	b	STA 1.1.3	K3	1
31	c	STA 1.1.1	K2	1
32	c	STA 2.2.1	K2	1
33	c	STA 3.3.1	K3	1
34	a	STA 5.2.1	K2	1
35	b	STA 6.1.1	K2	1
36	a, b	STA 3.1.2	K4	2
37	a	STA 3.2.1	K3	1
38	a	STA 3.2.2	K3	1
39	d	STA 3.1.1	K2	1
40	c	STA 6.2.1	K4	2

© International Software Testing Qualifications Board



Answers

© International Software Testing Qualifications Board



Question Number (#)	Correct Answer	Explanation / Rationale	Learning Objective (LO)	K-Level	Number of Points
1	d	a) Is not correct. It overemphasizes security vulnerability and threat linkage, but an asset is defined by value, not only by its exposure to threats. b) Is not correct. It is too narrow—focuses only on technical components and excludes intangible assets such as reputation, PII, or intellectual property. c) Is not correct. It incorrectly restricts assets to those formally documented, whereas assets exist regardless of documentation status. d) Is correct. It accurately reflects the definition from the syllabus and NIST: includes any data, device, system, or component, both tangible and intangible, that supports information-related activities and has value requiring protection.	STA 1.1.1	K2	1
2	c	a) Is not correct. Recreating or recovering an asset affects its value. b) Is not correct. Potential damage from asset loss impacts risk assessment. c) Is correct. Focuses on risk assessment context, but asset value is determined independently of threats and vulnerabilities. d) Is not correct. Legal liabilities influence the financial and operational risk impact of asset compromise.	STA 1.1.2	K2	1
3	a, c	a) Is correct. It represents a highly exploitable and testable security vulnerability, central to security testing. b) Is not correct. Important but not directly testable via penetration testing. c) Is correct. Directly affects encryption effectiveness, making it critical and testable. d) Is not correct. A process weakness, not an exploitable technical risk. e) Is not correct. Focuses on operational/environmental risk, not security exploitability.	STA 1.1.3	K3	1

© International Software Testing Qualifications Board



4	b	a) Is not correct. Asset replacement cost relates to risk impact, not likelihood of exploitation. b) Is correct. Ease of exploiting a vulnerability directly affects how likely a threat can succeed. c) Is not correct. The number of assets affects scope but does not directly influence the likelihood of exploitation. d) Is not correct. Risk appetite guides overall risk acceptance but does not determine threat exploitation likelihood.	STA 1.2.1	K2	1
5	a	a) Is correct. This best reflects anticipation + prioritization + tailoring of testing, which is the key benefit. b) Is not correct. This focuses on threat modeling, not the direct enhancement of test prioritization and test execution. c) Is not correct. It emphasizes risk assessment, not specifically testing improvement. d) Is not correct. It focuses on completeness, whereas the key idea is relevance and prioritization.	STA 2.1.1	K2	1

© International Software Testing Qualifications Board



6	a, c	a) Is correct. Attackers often use open-source intelligence techniques to gather information from publicly available sources. b) Is not correct. It involves interacting directly with systems, which can trigger alerts and is not aligned with passive reconnaissance attackers use to discover key information externally. c) Is correct. Job postings frequently contain technical details that can be valuable to attackers. Revealing technology stack and internal practices. d) Is not correct. While phishing is a common social engineering attack, this method is used to exploit information rather than gather it passively. It's part of an active exploitation phase and is more relevant to testing employee awareness or response, not initial reconnaissance. e) Is not correct. This is an internal security control and part of defensive security practices, not something an attacker would do during reconnaissance. It requires privileged access and is not a method attackers use to discover information externally. Appears passive, but DNS enumeration may involve interaction with target infrastructure, making it borderline active in this context.	STA 2.1.2	K3	1
7	c	a) Is not correct. Represents an indirect insider scenario, but primary exploitation is external. b) Is not correct. Mimics social trust but is external, lacking true internal access. c) Is correct. This combines technical access (via an internal account) with social trust factors, creating a significant insider risk. d) Is not correct. A negligent insider but lacks social exploitation element.	STA 2.2.1	K2	1

© International Software Testing Qualifications Board



8	b	a) Is not correct. Misusing privileges is more characteristic of insiders , who already have access. The claim that insiders "do not consider any context" is vague and inaccurate; insider often act with specific intent and knowledge of the environment. b) Is correct. External attackers typically try to exploit security vulnerabilities (e.g., in web servers, firewalls, or applications) to gain access. Insiders already have credentials and may abuse them to access areas or data they should not. c) Is not correct. This is misleading. It describes the opposite of typical behavior. External attackers usually try to bypass perimeter defenses (i.e. firewalls, authentication systems), while insiders may exploit weaknesses that are only visible or accessible after gaining authorized access. d) Is not correct. This mixes up roles. External attackers are the ones who typically probe public-facing assets (like websites or APIs) for vulnerabilities. Insiders are more likely to assess how internal defenses can be bypassed or misused from within the network.	STA 2.2.2	K2	1
9	a, e	a) Is correct. These parameters are relevant for possibly touched business processes and relevant rules b) Is not correct. Available budget does not have risk but possible risk treatments c) Is not correct. Risk management itself is agnostic from any tool involved. d) Is not correct. Technical parameters may influence *likelihood* later in analysis, they do not define the overall context in which risks are identified and evaluated. e) Is correct. Dependencies on **external suppliers** are part of the organization's external environment and can influence both the scope and the boundaries of risk management.	STA 3.1.1	K2	1

© International Software Testing Qualifications Board

10	c	a) Is not correct. Acceptance of identified risk in early development phases does not make any sense; based on the shift-left approach. The cost to mitigate these risks will increase over time. b) Is not correct. Risks are not related to specific roles or persons, but to the whole organization developing a product. c) Is correct. Security risks should be mitigated as early as possible. d) Is not correct. Risk avoidance generates a negative impact on business which is expecting the affected component; usually risk avoidance is only used as last-minute step before go-live.	STA 3.1.2	K4	2
11	a	a) Is correct. The internal control systems goal is to provide 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) Is not correct. Policies do not necessarily contain all regulative requirements. c) Is not correct. The internal control system's goal is not to provide any template for policies. d) Is not correct. This is because not all policies are necessarily based on any best practice.	STA 3.2.1	K3	1
12	d	a) Is not correct. This is because the security internal control systems do not define security test policies. b) Is not correct. This is because the security test analyst is not responsible for the internal control system. c) Is not correct. This is because the internal control system is not the masterplan for all security testing activities. d) Is correct. Most security testing activities should be related to the internal control system. This task has to be supported by the Security Test Analyst.	STA 3.2.2	K3	1

© International Software Testing Qualifications Board



13	a	a) Is correct. This Precisely applies regulations with explicit control activities and provides direct mapping from regulation to test cases. It also includes expected results and traceability, which are critical. b) Is not correct. It is strong and regulation-focused, but extends beyond explicit requirements. It introduces interpretation and expansion, which may reduce compliance precision. c) Is not correct. It validates effectiveness, but focuses on behavior rather than explicit regulatory checks. This may miss specific mandated control activities (e.g., reconciliation timing). d) Is not correct. This aligns with regulatory intent, but remains at principal level rather than concrete derivation. It lacks explicit one-to-one mapping to regulatory controls.	STA 3.3.1	K3	1
14	a	a) Is correct. This clearly differentiates the “what” (test objectives – goals like compliance or risk reduction) from the “how” (test strategy – plan and approach to achieve those goals). b) Is not correct. Reverses the concepts: test tools and test techniques belong to the test strategy, and compliance and assurance goals are part of the test objectives. c) Is not correct. Misrepresents both terms: test objectives are not “general guidelines,” and the test strategy covers far more than just compliance. d) Is not correct. It misrepresents the purpose of security test objectives by associating them with operational planning decisions, such as scheduling penetration tests and security vulnerability scans. In reality, test objectives focus on what security-related results or goals need to be achieved, for example validating compliance, identifying vulnerabilities, or assessing risk level.	STA 4.1.1	K2	1

© International Software Testing Qualifications Board



15	b	a) Analytical test strategy is not correct. Strength: Provides traceability from requirements to tests, addressing (point 3). Weakness: It does not provide regulatory compliance (point 1) and does not naturally integrate with CI/CD (point 4). Too narrow. b) Is correct. Process-compliant test strategy provides that testing is aligned with GDPR and PCI DSS (point 1). Regression-averse test strategy provides automated security vulnerability scans in each build (points 2 & 4). Together, they cover compliance, iterative development, traceability, and continuous feedback, making this the most comprehensive choice. c) Model based test strategy is not correct. Strength: Threat modeling addresses API misuse and evolving risks (point 2). Weakness: Fails compliance verification (point 1) and does not guarantee requirement traceability (point 3). Too risk-focused without compliance rigor. d) Reactive test strategy is not correct. Strength: Identifies vulnerabilities dynamically (point 2). Weakness: Too late — only detects defects after they appear, with no preventive or compliance assurance (point 1). It also does not fit CI/CD's need for continuous evidence (point 4).	STA 4.1.2	K3	1

© International Software Testing Qualifications Board



16	a	a) Is correct. The scenario focuses on newly integrated third-party libraries and implementation-related weaknesses during development. SCA is specifically used to identify vulnerable or outdated open-source and third-party components, while SAST analyzes source code for security weaknesses during implementation. Both activities belong to incremental security verification activities and support early security vulnerability detection before system testing begins. b) Is not correct. Penetration testing is typically performed during pre-release security validation phases after the system has been fully integrated and stabilized. Its purpose is to simulate realistic attacks against the operational application. The scenario, however, requires early detection of vulnerabilities during implementation activities. c) Is not correct. Operational security monitoring is a post-deployment activity focused on detecting failures, monitoring threats, and maintaining compliance during production operations. The application in this scenario has not yet entered system testing or production. d) Threat modeling is primarily performed during design and architectural review phases to identify attack vectors, trust boundaries, and misuse cases before implementation begins. In this scenario, implementation activities are already underway and the focus is on identifying vulnerabilities in code and integrated software components.	STA 4.2.1	K3	1
17	d	a) Is not correct. b) Is not correct. c) Is not correct. d) Is correct. Metric: Measures to track progress of executing a WP Resources: Financial expenses required to undertake a WP Dependency: Reliance of one WP with other tasks or WPs Scope: Explicit definition of what is included and excluded in the WP	STA 5.1.1	K2	1

© International Software Testing Qualifications Board



18	b	a) Is not correct. While common, the text states that general formulations like OWASP Top 10 are easy to make but leave many other aspects unspecified and may not meet specific regulatory needs. b) Is correct. The text suggests that since manual security testing time is unpredictable, prioritizing and time-boxing are effective strategies to manage these uncertainties. c) Is not correct. The text explicitly mentions that security testing requires specific competencies and know-how, even for tasks like configuring security vulnerability scanning tools. d) Is not correct. Although many organizations do this, the text identifies late integration as a challenge rather than a recommended best practice for effective risk mitigation.	STA 5.1.2	K3	1
19	b	a) Is not correct. This is because while budget is mentioned in the text, it is associated with "procuring authorizations and approvals," not specifically with the scheduling and estimation of tasks. b) Is correct. This is because the text explicitly lists "Which security-related items need to be implemented and tested before other testing occurs" under planning the schedule, and "Time needed to perform regression tests" under defining and estimating activities. c) Is not correct. This is because outsourcing considerations fall under "identifying who should perform the security tests," rather than the scheduling or estimation of specific tasks. d) Is not correct. This is because defining the platform and technology refers to "defining the security test environment," which is a separate planning aspect from task estimation and scheduling.	STA 5.2.1	K2	1
20	d	a) Is not correct. Specifying of work packages is not mentioned. b) Is not correct. It does not consider combining system elements in a single work package. c) Is not correct. It is mentioning only tooling. d) Is correct. This is the most complete, generic and correct answer.	STA 5.2.2	K3	1

© International Software Testing Qualifications Board



21	c, e	a) Is not correct. Budget controlling should not be part of any test report. b) Is not correct. Frequency of test execution is irrelevant for a test report. c) Is correct. This is because the intended audience defines the level of details of a test report. d) Is not correct. The skills of the test engineer should not be part of any test report. e) Is correct. This is because the level of confidentiality is essential for all recipients of a test report.	STA 6.1.1	K2	1

© International Software Testing Qualifications Board



22	a, d	a) Is correct. Explanation of very technical aspects to non-IT stakeholders. Managing security test reports requires communicating findings to different audiences, including management and non-technical stakeholders. Translating technical results into business-relevant language is explicitly part of the STA's test report-related responsibilities in the syllabus section on test-result interpretation and follow-ups. This supports timely decisions about risk and action planning and squarely fits the "manage … test reports" phrasing (communication is central to management of test reports). b) Is not correct. Suggestion for and consulting for possible mitigation actions- Advising on mitigations is indeed mentioned in the syllabus as something an STA can do; however, the stem narrows scope to "manage security test reports." Within that narrower focus, the two most essential capabilities are (1) communication of test report content and (2) providing correct classification/priority so follow-up is managed. c) Is not correct. Implementation of mitigation actions. Actually, doing the fixes is not part of the STA's role. Implementation belongs to developers/security test engineers; the STA analyzes, communicates, classifies, and tracks. The syllabus' roles/structure make this separation clear. Thus, this option conflicts with expected STA responsibilities. d) Is correct. Support of severity classification. Severity/priority classification of findings is a core piece of managing a security test report: it drives which items are escalated, timelines, and follow-up tracking. The syllabus text for 6.1.2 explicitly calls out the STA's role in supporting severity classification, so vulnerabilities are mitigated in a timely manner. This is directly tied to "managing" test reports and their follow-ups. e) Is not correct. Identification of skilled people and organizing a task force is not part of Security Test Analyst's job description.	STA 6.1.2	K2	1

© International Software Testing Qualifications Board



23	b, d	a) Is not correct. The Security Test Analyst (STA) is not responsible for directly fixing vulnerabilities. Fixing and confirmation testing are handled by the Security Test Engineer and developers. The STA's role is to analyze the test results, prioritize actions, and communicate risk impact to management, after that the communication with developer can start. b) Is correct. Creating a management-level summary that highlights risk level and implications for the planned go-live. This supports management's decision-making process on whether to delay or proceed with release. c) Is not correct. While joint analysis between STA, STE, and developers is appropriate, the communication path here is wrong: the STA consolidates the test report, not the STE. The STE does not independently send mitigation proposals to management. d) Is correct. Preparing a structured decision template allows management to assess risk acceptance, transfer, or mitigation options. The STA transforms findings into actionable decisions. e) Is not correct. Simply forwarding the test report without analysis or prioritization does not satisfy the STA's responsibility. It shows no analytical or communicative value-add, failing the intent.	STA 6.2.1	K4	2
24	a	a) Is correct. Clearly represents active reconnaissance, directly interacting with systems to map the attack surface, which is the stated objective. b) Is not correct. Represents active exploitation (phishing), not reconnaissance. c) Is not correct. This is passive reconnaissance (DNS/OSINT), not active. d) Is not correct. Represents threat intelligence analysis, not active reconnaissance against the target.	STA 2.1.2	K3	1

© International Software Testing Qualifications Board



25	a	a) Is correct. This answer correctly applies to the distinction: test objectives describe what must be achieved, whereas the test strategy describes how those test objectives will be reached in the given context. b) Is not correct. Selecting test types (e.g. penetration testing, security vulnerability scanning) is part of the security test strategy, while proving compliance and resilience are security test objectives. c) Is not correct. While test objectives are high-level goals, translating them into detailed test cases and scripts is part of test design and implementation, not the definition of the security test strategy itself. d) Is not correct. Both test objectives and test strategy are defined before testing begins. The difference lies in purpose and content, not in when they are defined.	STA 4.1.1	K2	1
26	a	a) Is correct. Analytical test strategies, particularly risk-based testing, are the right approach when test design is driven by risks and requirements. b) Is not correct. A methodical checklist provides coverage of known vulnerabilities but does not prioritize tests based on specific risks to this platform. c) Is not correct. This helps detect newly introduced weaknesses but doesn't address prioritizing security risks identified during requirements and risk analysis. d) Is not correct. Customer input may add context, but it lacks the systematic, requirements- and risk-driven approach needed in this scenario.	STA 4.1.2	K3	1

© International Software Testing Qualifications Board



27	b	a) Is not correct. Continuous security monitoring is an operational. security activity performed after deployment or during production operations. Its purpose is to identify newly emerging threats, detect incidents, and support ongoing compliance through activities such as log analysis, security vulnerability scanning, and security auditing. The scenario, however, focuses on identifying threats and trust boundaries before release integration. b) Is correct. The scenario explicitly describes activities such as identifying attack vectors, analyzing trust boundaries, evaluating sensitive data flows, and defining misuse cases. These are core elements of threat modeling and security design reviews. These activities are typically performed during feature design or before implementation is finalized in order to proactively identify and mitigate architectural and design-related security risks. c) Is not correct. Penetration testing is generally conducted during pre-release security validation phases after the system or feature has already been implemented and integrated. Its objective is to simulate realistic attacks against the operational system to identify exploitable vulnerabilities. In this scenario, the focus is still on early identification of design-related threats before integration. d) Is not correct. DAST is a runtime security verification activity executed against a running application during integration or system testing. It is used to identify vulnerabilities in implemented functionality. The scenario, however, addresses the analysis of architectural risks and attack surfaces before the feature reaches later verification phases.	STA 4.2.1	K3	1

© International Software Testing Qualifications Board



28	a	a) Is correct. Combining all identical test types to be most effective b) Is not correct. Defining a work package for each test object does not utilize the possible positive effect from work packages. c) Is not correct. Performing a risk assessment for each test object should be done before defining work packages. d) Is not correct. Prioritizing the sequence of work package execution should be done after having defined the work packages.	STA 5.1.2	K3	1
29	d	a) Is not correct. Context of the testing because it is important to identify and specify what will be tested. b) Is not correct. Risk register because it will create a complete overview for the whole system. c) Is not correct. Test strategy as it will describe all necessary details for the security testing. d) Is correct. Schedule as this will show which work package shall be executed based on different parameters.	STA 5.2.2	K3	1
30	b	a) Is not correct. This is a valid security weakness (key management issue) affecting confidentiality, but it lacks a clear exploitation path and dependency chain compared to B, making it less critical in this context. b) Is correct. This demonstrates a multi-step attack path across dependent assets (portal → privilege escalation → backend → PII), aligning strongly with BIA dependency analysis and high-impact data breach risk. c) Is not correct. This represents a data integrity/availability issue with limited exposure conditions, but the likelihood and direct exploitability are lower than a privilege escalation scenario. d) Is not correct. This focuses on performance degradation, not a direct compromise of a protected asset.	STA 1.1.3	K3	1

© International Software Testing Qualifications Board



31	c	a) Is not correct. Completing training is a personnel security measure and does not change the status of hardware or software assets. b) Is not correct. A security vulnerability scan uses the asset inventory to know what to scan. While the results of a scan might reveal an unknown asset (which would then force an update), the mere schedule of the scan is not the trigger for updating the register. c) Is correct. Asset management is a lifecycle process, not just a static list. The inventory is a "living" record. An update is strictly required whenever the status of an asset changes—this includes acquisition (birth), transfer of custody or location (life), and disposal (death). Without updating the inventory at these specific moments, the organization cannot effectively manage risk or patch levels. d) Is not correct. Budget reviews are financial processes. While they rely on asset data, the act of reviewing the budget does not trigger a change in the asset database itself.	STA 1.1.1	K2	1
32	c	a) Is not correct. This describes a Malicious Insider (specifically theft/espionage) where there is clear intent to harm or profit. b) Is not correct. While this is an internal breach, is classified as curiosity-driven access or policy violation with intent as a form of intentional misconduct (often labeled "The Goof" or simply unauthorized access) rather than a pure "accident" or "carelessness" in the context of phishing/malware. c) Is correct. The Careless/Accidental Insider is an example of where a significant portion of internal threats are not malicious but accidental. The "Careless Employee" is described as a legitimate user who, often through lack of training or simple error (like clicking on a phishing link), exposes the organization to risk without any intent to cause harm. d) Is not correct: This describes a Malicious Insider (or potentially a compromised vendor acting maliciously), as the action of modifying privileges is intentional and unauthorized.	STA 2.2.1	K2	1

© International Software Testing Qualifications Board



33	c	a) Is not correct. It emphasizes consistency and coverage, but remains process-oriented. It is missing specific compliance checks tied to regulation thresholds. b) Is not correct. This has a strong regulatory alignment, but focuses on assessment rather than explicit verification criteria. It lacks precise measurable expected results. c) Is correct. It correctly converts regulation to measurable test cases with expected results. and enables objective pass/fail evaluation (≤12 months, ≤90 days). d) Is not correct. This evaluates effectiveness of processes, but does not directly verify regulatory conditions. It risks indirect compliance validation instead of explicit confirmation.	STA 3.3.1	K3	1
34	a	a) Is correct. Scope Definition is about establishing the boundaries of the test. It answers the question "What are we testing?" By listing exactly which assets (IPs, apps) are included and which are excluded, the manager is defining the scope. b) Is not correct. Risk Assessment is the process of identifying risks before the test to determine why the test is needed, but it does not define the specific targets of the test itself. c) Is not correct. Rules of Engagement (RoE) define how the test is performed (e.g., "Do not use social engineering" or "Stop if you find PII"). While scope is often attached to RoE, listing the targets and exclusions is specifically a scoping activity. d) Is not correct. Test reporting requirements define how the results should be delivered (e.g., "We need a PDF test report within 5 days"), not which systems are being tested.	STA 5.2.1	K2	1

© International Software Testing Qualifications Board



35	b	a) Is not correct. The scenario states the test report contained code snippets and requests (evidence), so Proof of Concept was likely present; the issue was that the Board couldn't understand it. b) Is correct. Effective security communication requires tailoring the test report to the specific audience. A Board of Directors is a non-technical audience focused on business risk, financial loss, and reputation. A test report that lacks a non-technical Executive Summary translating technical defects into business language fails to communicate effectively, even if the data is accurate. c) Is not correct. The test report actually contained too much technical detail (raw logs/code), so the problem wasn't a lack of data for IT, but rather the inclusion of that data for the wrong audience. d) Is not correct. While methodology is important, the Board's rejection was based on their inability to use the data for decision-making (business impact), not a concern over which tools were used.	STA 6.1.2	K2	1
36	a, b	a) Is correct. Represents risk evaluation, incorporating business context, which is the next required step. b) Is correct. Supports communication and consultation, enabling informed evaluation and treatment decisions. c) Is not correct. Valuable, but remains within analysis, not progressing the lifecycle. d) Is not correct. Reasonable but leans into treatment prematurely, before formal evaluation is completed. e) Is not correct. Expands scope of identification, not advancing methodological progression.	STA 3.1.2	K4	2

© International Software Testing Qualifications Board



37	a	a) Is correct. Captures the core ICS principle: policies must be converted into testable controls with feedback mechanisms. b) Is not correct. Very strong—includes traceability, but does not explicitly provide testable validation derived from policies. c) Is not correct. Focuses on continuous improvement, but not the initial policy-to-control transformation. d) Is not correct. Addresses coordination and efficiency, but not policy-driven control definition and validation.	STA 3.2.1	K3	1
38	a	a) Is correct. This directly applies spot checks and alignment verification. Includes adjustment of policy, system, and tests. And is fully aligned with continuous ICS improvement. b) Is not correct. This expands coverage appropriately, but may miss misalignment with policy. It focuses on tests, but not overall control system alignment. c) Is not correct. This improves detection probability, but not effectiveness of outdated tests. Repetition does not fix structural misalignment. d) Is not correct. This has strong preventive control, but does not address existing misalignment. It lacks direct validation of current control effectiveness.	STA 3.2.2	K3	1

© International Software Testing Qualifications Board



39	d	a) Is not correct. It suggests alignment and monitoring, but lacks explicit continuous improvement as a defined step. Treatment is described generically, not clearly reflecting systematic treatment options. b) Is not correct. Focuses strongly on mitigation as primary treatment. Communication and improvement are weakened (periodic, not continuous). c) Is not correct. Omits explicit emphasis on continuous monitoring and improvement and uses “periodic evaluation,” which weakens active risk management principle. d) Is correct. This Explicitly includes all five ISO 31000 elements of Establishing the context, Risk assessment, Risk treatment, Communication and consultation, and Continuous process improvement. It also clearly reflects complete and continuous methodology.	STA 3.1.1	K2	1
40	c	a) Is not correct. Transport Layer Security (TLS) update is important but less urgent compared to a critical exploit. b) Is not correct. Security headers are important but less urgent compared to a critical exploit. c) Is correct. SQL Injection with a CVSS score of 9.8 (Critical) poses the highest risk because it can lead to full database compromise. d) Is not correct. Deferring fixes ignores the immediate threat.	STA 6.2.1	K4	2

© International Software Testing Qualifications Board