Standard Glossary of Terms used in Software Testing

Version 3.1

Advanced Security Tester Terms

International Software Testing Qualifications Board

abuse case

See Also: use case

A use case in which some actors with malcious intent are causing harm to the system or to other actors.

acceptance criteria

Ref: IEEE 610

The exit criteria that a component or system must satisfy in order to be accepted by a user, customer, or other authorized entity.

account harvesting

The process of obtaining lists of email addresses for use in bulk email messages.

accuracy

Ref: ISO 9126 **See Also:** functionality

The capability of the software product to provide the right or agreed results or effects with the needed degree o precision.

actor

User or any other person or system that interacts with the test object in a specific way.

actual result

Synonyms: actual outcome

The behavior produced/observed when a component or system is tested.

anti-malware

Software that is used to detect and inhibit malware. See also malware.

API

Acronym for Application Programming Interface.

attack vector

A path or means by which an attacker can gain access to a system for malicious purposes.

attacker

See Also: hacker

A person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.

audit

Ref: IEEE 1028

An independent evaluation of software products or processes to ascertain compliance to standards, guidelines, specifications, and/or procedures based on objective criteria, including documents that specify: the form or content of the products to be produced, the process by which the products shall be produced, and how compliance to standards or guidelines shall be measured.

audit trail

Ref: After TMap

A path by which the original input to a process (e.g., data) can be traced back through the process, taking the process output as a starting point. This facilitates defect analysis and allows a process audit to be carried out.

authentication

See Also: authorization

A procedure determining whether a person or a process is, in fact, who or what it is declared to be.

authorization

See Also: authentication

Permission given to a user or process to access resources.

availability

Ref: IEEE 610

The degree to which a component or system is operational and accessible when required for use. Often expressed as a percentage.

baseline

Ref: After IEEE 610

A specification or software product that has been formally reviewed or agreed upon, that thereafter serves as the basis for further development, and that can be changed only through a formal change control process.

best practice

A superior method or innovative practice that contributes to the improved performance of an organization unde given context, usually recognized as "best" by other peer organizations.

botnet

A network of compromised computers, called bots or robots, which is controlled by a third party and used to transmit malware or spam, or to launch attacks.

branch coverage

The percentage of branches that have been exercised by a test suite. 100% branch coverage implies both 100% decision coverage and 100% statement coverage.

buffer overflow

See Also: buffer

A memory access failure due to the attempt by a process to store data beyond the boundaries of a fixed length buffer, resulting in overwriting of adjacent memory areas or the raising of an overflow exception.

change management

See Also: configuration management

(1) A structured approach to transitioning individuals and organizations from a current state to a desired future state. (2) Controlled way to effect a change, or a proposed change, to a product or service.

CLI

Acronym for Command-Line Interface.

code

Ref: IEEE 610

Computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler or other translator.

commercial off-the-shelf (COTS)

Synonyms: off-the-shelf software

A software product that is developed for the general market, i.e. for a large number of customers, and that is delivered to many customers in identical format.

compiler

Ref: IEEE 610

A software tool that translates programs expressed in a high-order language into their machine language equivalents.

complexity

See Also: cyclomatic complexity

The degree to which a component or system has a design and/or internal structure that is difficult to understand, maintain and verify.

compliance

Ref: ISO 9126

The capability of the software product to adhere to standards, conventions or regulations in laws and similar prescriptions.

---

component

Synonyms: module , unit

A minimal software item that can be tested in isolation.

---

component integration testing

Synonyms: link testing

Testing performed to expose defects in the interfaces and interaction between integrated components.

---

component testing

Ref: After IEEE 610

Synonyms: module testing , program testing , unit testing

The testing of individual software components.

---

computer forensics

The practice of determining how a security attack has succeeded and assessing the damage caused.

---

condition

See Also: condition testing

Synonyms: branch condition

A logical expression that can be evaluated as True or False, e.g., A>B.

---

configuration

The composition of a component or system as defined by the number, nature, and interconnections of its constituent parts.

---

configuration management

Ref: IEEE 610

A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

---

confirmation testing

Synonyms: re-testing

Testing that runs test cases that failed the last time they were run, in order to verify the success of corrective actions.

control flow

A sequence of events (paths) in the execution through a component or system.

control flow graph

An abstract representation of all possible sequences of events (paths) in the execution through a component or system.

coverage

Synonyms: test coverage

The degree, expressed as a percentage, to which a specified coverage item has been exercised by a test suite

cross-site scripting (XSS)

Ref: NIST.IR.7298

A vulnerability that allows attackers to inject malicious code into an otherwise benign website.

cyclomatic complexity

Ref: After McCabe

Synonyms: cyclomatic number

The maximum number of linear, independent paths through a program. Cyclomatic complexity may be computed as L = N + 2P, where L = the number of edges/links in a graph, N = the number of nodes in a graph, P = the number of disconnected parts of the graph (e.g., a called graph or subroutine).

dashboard

See Also: corporate dashboard, scorecard

A representation of dynamic measurements of operational performance for some organization or activity, using metrics represented via metaphors such as visual dials, counters, and other devices resembling those on the dashboard of an automobile, so that the effects of events or activities can be easily understood and related to operational goals.

data flow

Ref: Beiser

An abstract representation of the sequence and possible changes of the state of data objects, where the state of an object is any of creation, usage, or destruction.

data obfuscation

Data transformation that makes it difficult for a human to recognize the original data.

data privacy

The protection of personally identifiable information or otherwise sensitive information from undesired disclosure

data-driven testing

Ref: Fewster and Graham **See Also:** keyword-driven testing

A scripting technique that stores test input and expected results in a table or spreadsheet, so that a single control script can execute all of the tests in the table. Data-driven testing is often used to support the applicatior of test execution tools such as capture/playback tools.

debugging

The process of finding, analyzing and removing the causes of failures in software.

decision

A program point at which the control flow has two or more alternative routes. A node with two or more links to separate branches.

decision outcome

The result of a decision (which therefore determines the branches to be taken).

defect

Synonyms: bug , fault , problem

A flaw in a component or system that can cause the component or system to fail to perform its required function, e.g., an incorrect statement or data definition. A defect, if encountered during execution, may cause a failure of the component or system.

defect report

Ref: After IEEE 829

Synonyms: bug report , problem report

A document reporting on any flaw in a component or system that can cause the component or system to fail to perform its required function.

deliverable

Any (work) product that must be delivered to someone other than the (work) product's author.

demilitarized zone (DMZ)

See Also: network zone

A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, commonly the Internet.

denial of service (DOS)

A security attack that is intended to overload the system with requests such that legitimate requests cannot be serviced.

domain

The set from which valid input and/or output values can be selected.

driver

Ref: After TMap

Synonyms: test driver

A software component or test tool that replaces a component that takes care of the control and/or the calling of a component or system.

dynamic analysis tool

A tool that provides run-time information on the state of the software code. These tools are most commonly used to identify unassigned pointers, check pointer arithmetic and to monitor the allocation, use and de-allocation of memory and to flag memory leaks.

dynamic testing

Testing that involves the execution of the software of a component or system.

effectiveness

See Also: efficiency

The capability of producing an intended result.

efficiency

Ref: ISO 9126

(1) The capability of the software product to provide appropriate performance, relative to the amount of resources used, under stated conditions. (2) The capability of a process to produce the intended outcome, relative to the amount of resources used.

encryption

The process of encoding information so that only authorized parties can retrieve the original information, usually by means of a specific decryption key or process.

equivalence partition

Synonyms: equivalence class

A portion of an input or output domain for which the behavior of a component or system is assumed to be the same, based on the specification.

---

error

Ref: After IEEE 610

Synonyms: mistake

A human action that produces an incorrect result.

---

ethical hacker

A security tester using hacker techniques.

---

executable statement

A statement which, when compiled, is translated into object code, and which will be executed procedurally whe the program is running and may perform an action on data.

---

exercised

A program element is said to be exercised by a test case when the input value causes the execution of that element, such as a statement, decision, or other structural element.

---

exit criteria

Ref: After Gilb and Graham

Synonyms: completion criteria , test completion criteria

The set of generic and specific conditions, agreed upon with the stakeholders for permitting a process to be officially completed. The purpose of exit criteria is to prevent a task from being considered completed when there are still outstanding parts of the task which have not been finished. Exit criteria are used to report against and to plan when to stop testing.

---

expected result

Synonyms: expected outcome , predicted outcome

The behavior predicted by the specification, or another source, of the component or system under specified conditions.

---

fail

Synonyms: test fail

A test is deemed to fail if its actual result does not match its expected result.

---

failure

Ref: After Fenton

Deviation of the component or system from its expected delivery, service or result.

fault attack

See Also: negative testing, security attack

Synonyms: attack

Directed and focused attempt to evaluate a specific quality characteristic of a test object by attempting to force specific failures to occur. Usually focused on reliability or security.

feature

Ref: After IEEE 1008

Synonyms: software feature

An attribute of a component or system specified or implied by requirements documentation (for example reliability, usability or design constraints).

firewall

A component or set of components that controls incoming and outgoing network traffic based on predetermined security rules.

functional requirement

Ref: IEEE 610

A requirement that specifies a function that a component or system must perform.

functional testing

See Also: black-box testing

Testing based on an analysis of the specification of the functionality of a component or system.

functionality

Ref: ISO 9126

The capability of the software product to provide functions which meet stated and implied needs when the software is used under specified conditions.

fuzz testing

Synonyms: fuzzing

A software testing technique used to discover security vulnerabilities by inputting massive amounts of random data, called fuzz, to the component or system.

GUI

Acronym for Graphical User Interface.

hacker

See Also: attacker

A person or organization who is actively involved in security attacks, usually with malicious intent.

hashing

Transformation of a variable length string of characters into a usually shorter fixed-length value or key. Hashed values, or hashes, are commonly used in table or database lookups. Cryptographic hash functions are used to secure data.

incident

Ref: After IEEE 1008

Synonyms: deviation , software test incident , test incident

Any event occurring that requires investigation.

incident management

Ref: After IEEE 1044

The process of recognizing, investigating, taking action and disposing of incidents. It involves logging incidents, classifying them and identifying the impact.

incident report

Ref: After IEEE 829

Synonyms: deviation report , software test incident report , test incident report

A document reporting on any event that occurred, e.g., during the testing, which requires investigation.

indicator

Ref: ISO 14598

A measure that can be used to estimate or predict another measure.

information assurance

Ref: NIST.IR.7298

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

information security

Ref: NIST.IR.7298

Synonyms: cybersecurity

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

input

A variable (whether stored within a component or outside) that is read by a component.

insider threat

A security threat originating from within the organization, often by an authorized system user.

inspection

Ref: After IEEE 610, IEEE 1028 **See Also:** peer review

A type of peer review that relies on visual examination of documents to detect defects, e.g., violations of development standards and non-conformance to higher level documentation. The most formal review technique and therefore always based on a documented procedure.

integration

The process of combining components or systems into larger assemblies.

integration testing

See Also: component integration testing, system integration testing

Testing performed to expose defects in the interfaces and in the interactions between integrated components o systems.

intrusion detection system (IDS)

See Also: malware scanning

A system which monitors activities on the 7 layers of the OSI model from network to application level, to detect violations of the security policy.

lifecycle model

Ref: CMMI **See Also:** software lifecycle

A partitioning of the life of a product or project into phases.

maintenance

Ref: IEEE 1219

Modification of a software product after delivery to correct defects, to improve performance or other attributes, or to adapt the product to a modified environment.

malware

Software that is intended to harm a system or its components.

malware scanning

See Also: intrusion detection system

Static analysis aiming to detect and remove malicious code received at an interface.

measure

Ref: ISO 14598

The number or category assigned to an attribute of an entity by making a measurement.

metric

Ref: ISO 14598

A measurement scale and the method used for measurement.

milestone

A point in time in a project at which defined (intermediate) deliverables and results should be ready.

model-based testing (MBT)

Testing based on or involving models.

network zone

A sub-network with a defined level of trust. For example, the Internet or a public zone would be considered to be untrusted.

open source tool

A software tool that is available to all potential users in source code form, usually via the internet. Its users are permitted, usually under license, to study, change, improve and, at times, to distribute the software.

operational environment

Hardware and software products installed at users' or customers' sites where the component or system under test will be used. The software may include operating systems, database management systems, and other applications.

output

A variable (whether stored within a component or outside) that is written by a component.

pass

Synonyms: test pass

A test is deemed to pass if its actual result matches its expected result.

password cracking

Ref: after NIST.IR.7298

A security attack recovering secret passwords stored in a computer system or transmitted over a network.

path

Synonyms: control flow path

A sequence of events, e.g., executable statements, of a component or system from an entry point to an exit point.

path coverage

The percentage of paths that have been exercised by a test suite. 100% path coverage implies 100% LCSAJ coverage.

path testing

A white-box test design technique in which test cases are designed to execute paths.

penetration testing

A testing technique aiming to exploit security vulnerabilities (known or unknown) to gain unauthorized access.

performance

Ref: After IEEE 610 **See Also:** efficiency

Synonyms: time behavior

The degree to which a system or component accomplishes its designated functions within given constraints regarding processing time and throughput rate.

performance indicator

Ref: CMMI

Synonyms: key performance indicator

A high-level metric of effectiveness and/or efficiency used to guide and control progressive development, e.g., lead-time slip for software development.

pharming

A security attack intended to redirect a web site's traffic to a fraudulent web site without the user's knowledge or consent.

phishing

An attempt to acquire personal or sensitive information by masquerading as a trustworthy entity in an electronic communication.

postcondition

Environmental and state conditions that must be fulfilled after the execution of a test or test procedure.

priority

The level of (business) importance assigned to an item, e.g., defect.

process

Ref: ISO 12207

A set of interrelated activities, which transform inputs into outputs.

process improvement

Ref: CMMI

A program of activities designed to improve the performance and maturity of the organization's processes, and the result of such a program.

process model

A framework wherein processes of the same nature are classified into a overall model, e.g., a test improvemen model.

project

Ref: ISO 9000

A project is a unique set of coordinated and controlled activities with start and finish dates undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources.

quality assurance

Ref: ISO 9000

Part of quality management focused on providing confidence that quality requirements will be fulfilled.

reconnaissance

Synonyms: footprinting

The exploration of a target area aiming to gain information that can be useful for an attack.

regression testing

Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made. It is performed when the software or its environment is changed.

requirement

Ref: After IEEE 610

A condition or capability needed by a user to solve a problem or achieve an objective that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed document.

requirements management tool

A tool that supports the recording of requirements, requirements attributes (e.g., priority, knowledge responsible) and annotation, and facilitates traceability through layers of requirements and requirements change management. Some requirements management tools also provide facilities for static analysis, such as consistency checking and violations to pre-defined requirements rules.

requirements-based testing

An approach to testing in which test cases are designed based on test objectives and test conditions derived from requirements, e.g., tests that exercise specific functions or probe non-functional attributes such as reliability or usability.

result

See Also: actual result, expected result

Synonyms: outcome , test outcome , test result

The consequence/outcome of the execution of a test. It includes outputs to screens, changes to data, reports, and communication messages sent out.

review

Ref: After IEEE 1028

An evaluation of a product or project status to ascertain discrepancies from planned results and to recommend improvements. Examples include management review, informal review, technical review, inspection, and walkthrough.

risk

A factor that could result in future negative consequences.

risk analysis

The process of assessing identified project or product risks to determine their level of risk, typically by estimating their impact and probability of occurrence (likelihood).

risk assessment

See Also: product risk, project risk, risk, risk impact, risk level, risk likelihood

The process of identifying and subsequently analyzing the identified project or product risk to determine its level of risk, typically by assigning likelihood and impact ratings.

risk identification

The process of identifying risks using techniques such as brainstorming, checklists and failure history.

risk impact

Synonyms: impact

The damage that will be caused if the risk becomes an actual outcome or event.

risk level

Synonyms: risk exposure

The importance of a risk as defined by its characteristics impact and likelihood. The level of risk can be used to determine the intensity of testing to be performed. A risk level can be expressed either qualitatively (e.g., high, medium, low) or quantitatively.

risk likelihood

Synonyms: likelihood

The estimated probability that a risk will become an actual outcome or event.

risk management

Systematic application of procedures and practices to the tasks of identifying, analyzing, prioritizing, and controlling risk.

risk mitigation

Synonyms: risk control

The process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels.

root cause analysis

An analysis technique aimed at identifying the root causes of defects. By directing corrective measures at root causes, it is hoped that the likelihood of defect recurrence will be minimized.

salting

See Also: hashing

A cryptographic technique that adds random data (salt) to the user data prior to hashing.

scalability

Ref: After Gerrard

The capability of the software product to be upgraded to accommodate increased loads.

script kiddie

See Also: hacker

A person who executes security attacks that have been created by other hackers rather than creating own ones.

security

Ref: ISO 9126 **See Also:** functionality

Attributes of software products that bear on its ability to prevent unauthorized access, whether accidental or deliberate, to programs and data.

security attack

Ref: after NIST.IR.7298

An attempt to gain unauthorized access to a system or component, resources, information, or an attempt to compromise system integrity.

security audit

An audit evaluating an organization's security processes and infrastructure.

security policy

A high-level document describing the principles, approach and major objectives of the organization regarding security.

security procedure

A set of steps required to implement the security policy and the steps to be taken in response to a security incident.

security testing

See Also: functionality testing

Testing to determine the security of the software product.

security testing tool

A tool that provides support for testing security characteristics and vulnerabilities.

security tool

A tool that supports operational security.

security vulnerability

A weakness in the system that could allow for a successful security attack.

severity

Ref: After IEEE 610

The degree of impact that a defect has on the development or operation of a component or system.

social engineering

Ref: NIST.IR.7298

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

software

Ref: IEEE 610

Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system.

software lifecycle

The period of time that begins when a software product is conceived and ends when the software is no longer available for use. The software lifecycle typically includes a concept phase, requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase, and sometimes, retirement phase. Note these phases may overlap or be performed iteratively.

specification

Ref: After IEEE 610

A document that specifies, ideally in a complete, precise and verifiable manner, the requirements, design, behavior, or other characteristics of a component or system, and, often, the procedures for determining whethe these provisions have been satisfied.

SQL injection

A security attack inserting malicious SQL statements into an entry field for execution.

stability

Ref: ISO 9126 **See Also:** maintainability

The capability of the software product to avoid unexpected effects from modifications in the software.

standard

Ref: After CMMI

Formal, possibly mandatory, set of requirements developed and used to prescribe consistent approaches to the way of working or to provide guidelines (e.g., ISO/IEC standards, IEEE standards, and organizational standards).

state transition

A transition between two states of a component or system.

statement

Synonyms: source statement

An entity in a programming language, which is typically the smallest indivisible unit of execution.

statement coverage

The percentage of executable statements that have been exercised by a test suite.

static analysis

Analysis of software development artifacts, e.g., requirements or code, carried out without execution of these software development artifacts. Static analysis is usually carried out by means of a supporting tool.

static analyzer

Synonyms: analyzer , static analysis tool

A tool that carries out static analysis.

static testing

Testing of a software development artifact, e.g., requirements, design or code, without execution of these artifacts, e.g., reviews or static analysis.

stub

Ref: After IEEE 610

A skeletal or special-purpose implementation of a software component, used to develop or test a component that calls or is otherwise dependent on it. It replaces a called component.

system

Ref: IEEE 610

A collection of components organized to accomplish a specific function or set of functions.

system hardening

The step-by-step process of reducing the security vulnerabilities of a system by applying a security policy and different layers of protection.

system integration testing

Testing the integration of systems and packages; testing interfaces to external organizations (e.g., Electronic Data Interchange, Internet).

system of systems

Multiple heterogeneous, distributed systems that are embedded in networks at multiple levels and in multiple interconnected domains, addressing large-scale inter-disciplinary common problems and purposes, usually without a common management structure.

system testing

Ref: Hetzel

Testing an integrated system to verify that it meets specified requirements.

technical review

Ref: Gilb and Graham, IEEE 1028 **See Also:** peer review

A peer group discussion activity that focuses on achieving consensus on the technical approach to be taken.

test

Ref: IEEE 829

A set of one or more test cases.

test analysis

The process of analyzing the test basis and defining test objectives.

test approach

The implementation of the test strategy for a specific project. It typically includes the decisions made that follow based on the (test) project's goal and the risk assessment carried out, starting points regarding the test process, the test design techniques to be applied, exit criteria and test types to be performed.

test architect

(1) A person who provides guidance and strategic direction for a test organization and for its relationship with other disciplines. (2) A person who defines the way testing is structured for a given system, including topics such as test tools and test data management.

test basis

Ref: After TMap

All documents from which the requirements of a component or system can be inferred. The documentation on which the test cases are based. If a document can be amended only by way of formal amendment procedure, then the test basis is called a frozen test basis.

test case

Ref: After IEEE 610

A set of input values, execution preconditions, expected results and execution postconditions, developed for a particular objective or test condition, such as to exercise a particular program path or to verify compliance with a specific requirement.

test closure

See Also: test process

During the test closure phase of a test process data is collected from completed activities to consolidate experience, testware, facts and numbers. The test closure phase consists of finalizing and archiving the testware and evaluating the test process, including preparation of a test evaluation report.

test condition

Synonyms: test requirement , test situation

An item or event of a component or system that could be verified by one or more test cases, e.g., a function, transaction, feature, quality attribute, or structural element.

test data

Data that exists (for example, in a database) before a test is executed, and that affects or is affected by the component or system under test.

test environment

Ref: After IEEE 610

Synonyms: test bed , test rig

An environment containing hardware, instrumentation, simulators, software tools, and other support elements needed to conduct a test.

test execution tool

A type of test tool that is able to execute other software using an automated test script, e.g., capture/playback.

test implementation

The process of developing and prioritizing test procedures, creating test data and, optionally, preparing test harnesses and writing automated test scripts.

test input

The data received from an external source by the test object during test execution. The external source can be hardware, software or human.

---

test management tool

A tool that provides support to the test management and control part of a test process. It often has several capabilities, such as testware management, scheduling of tests, the logging of results, progress tracking, incident management and test reporting.

---

test manager

Synonyms: test leader

The person responsible for project management of testing activities and resources, and evaluation of a test object. The individual who directs, controls, administers, plans and regulates the evaluation of a test object.

---

test object

See Also: test item

Synonyms: system under test

The component or system to be tested.

---

test objective

A reason or purpose for designing and executing a test.

---

test plan

Ref: After IEEE 829

A document describing the scope, approach, resources and schedule of intended test activities. It identifies amongst others test items, the features to be tested, the testing tasks, who will do each task, degree of tester independence, the test environment, the test design techniques and entry and exit criteria to be used, and the rationale for their choice, and any risks requiring contingency planning. It is a record of the test planning process.

---

test planning

The activity of establishing or updating a test plan.

---

test policy

A high-level document describing the principles, approach and major objectives of the organization regarding testing.

---

test procedure specification

Ref: After IEEE 829 **See Also:** test specification

Synonyms: test procedure , test scenario

A document specifying a sequence of actions for the execution of a test. Also known as test script or manual test script.

---

test process

The fundamental test process comprises test planning and control, test analysis and design, test implementation and execution, evaluating exit criteria and reporting, and test closure activities.

---

test reporting

See Also: test process

Collecting and analyzing data from testing activities and subsequently consolidating the data in a report to inform stakeholders.

---

test script

Commonly used to refer to a test procedure specification, especially an automated one.

---

test specification

A document that consists of a test design specification, test case specification and/or test procedure specification.

---

test strategy

A high-level description of the test levels to be performed and the testing within those levels for an organization or programme (one or more projects).

---

test tool

Ref: TMap **See Also:** CAST

A software product that supports one or more test activities, such as planning and control, specification, building initial files and data, test execution and test analysis.

---

test type

Ref: After TMap

A group of test activities aimed at testing a component or system focused on a specific test objective, i.e. functional test, usability test, regression test etc. A test type may take place on one or more test levels or test phases.

---

testability

Ref: ISO 9126 **See Also:** maintainability

The capability of the software product to enable modified software to be tested.

tester

A skilled professional who is involved in the testing of a component or system.

testing

The process consisting of all lifecycle activities, both static and dynamic, concerned with planning, preparation and evaluation of software products and related work products to determine that they satisfy specified requirements, to demonstrate that they are fit for purpose and to detect defects.

understandability

Ref: ISO 9126 **See Also:** usability

The capability of the software product to enable the user to understand whether the software is suitable, and how it can be used for particular tasks and conditions of use.

usability

Ref: ISO 9126

The capability of the software to be understood, learned, used and attractive to the user when used under specified conditions.

use case

A sequence of transactions in a dialogue between an actor and a component or system with a tangible result, where an actor can be a user or anything that can exchange information with the system.

validation

Ref: ISO 9000

Confirmation by examination and through provision of objective evidence that the requirements for a specific intended use or application have been fulfilled.

variable

An element of storage in a computer that is accessible by a software program by referring to it by a name.

verification

Ref: ISO 9000

Confirmation by examination and through provision of objective evidence that specified requirements have been fulfilled.

vulnerability scanner

A static analyzer that is used to detect particular security vulnerabilities in the code.

walkthrough

Ref: Freedman and Weinberg, IEEE 1028 **See Also:** peer review

Synonyms: structured walkthrough

A step-by-step presentation by the author of a document in order to gather information and to establish a common understanding of its content.

white-box testing

Synonyms: clear-box testing , code-based testing , glass-box testing , logic-coverage testing , logic-driven testing , structural testing , structure-based testing

Testing based on an analysis of the internal structure of the component or system.