# ISTQB – Foundation Level



## CHAPTER 5: TEST MANAGMENT

**Prepared by: Vu Nguyen**

**June 2010**

# AGENDA



- 5.1 Test organization (K2)
- 5.2 Test planning and estimation (K2)
- 5.3 Test progress monitoring and control (K2)
- 5.4 Configuration management (K2)
- 5.5 Risk and testing (K2)
- 5.6 Incident Management (K3)

# 5.1 Test organization (K2)

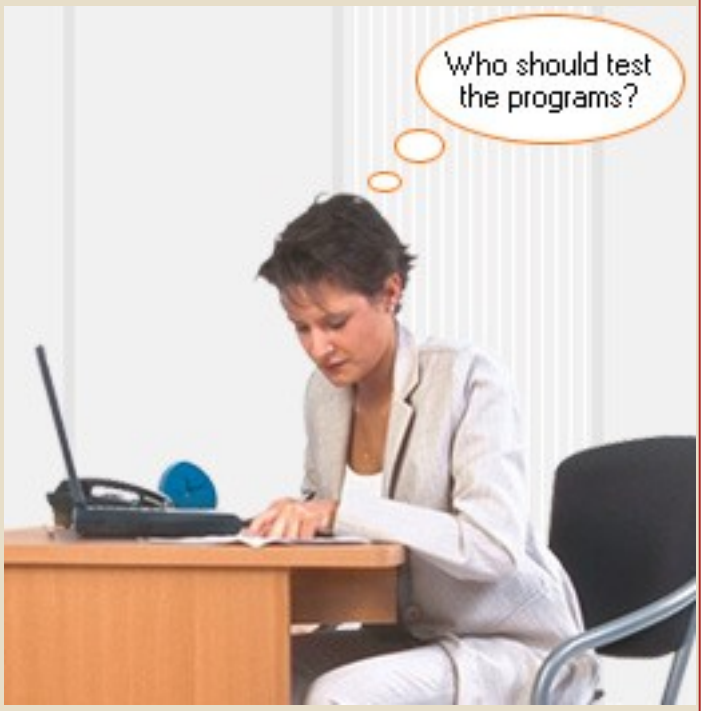


- Objectives
  - LO-5.1.1 Recognize the importance of independent testing. (K1)
  - LO-5.1.2 List the benefits and drawbacks of independent testing within an organization. (K2)
  - LO-5.1.3 Recognize the different team members to be considered for the creation of a test team.
  - (K1)
  - LO-5.1.4 Recall the tasks of typical test leader and tester. (K1)

# Independent and integrated testing



- The effectiveness of finding defects can be improved by using independent testers.
- Options for independence are:
  - No independent testers. Developers test their own code.
  - Independent testers within the development teams.
  - Independent test team or group within the organization.
  - Independent testers outsourced or external to the organization.



# Independent and integrated testing



- Other Options for independence are:
  - Independent testers from the business organization or user community.
  - Independent test specialists such as usability testers, security testers or certification testers.

# Independent and integrated testing

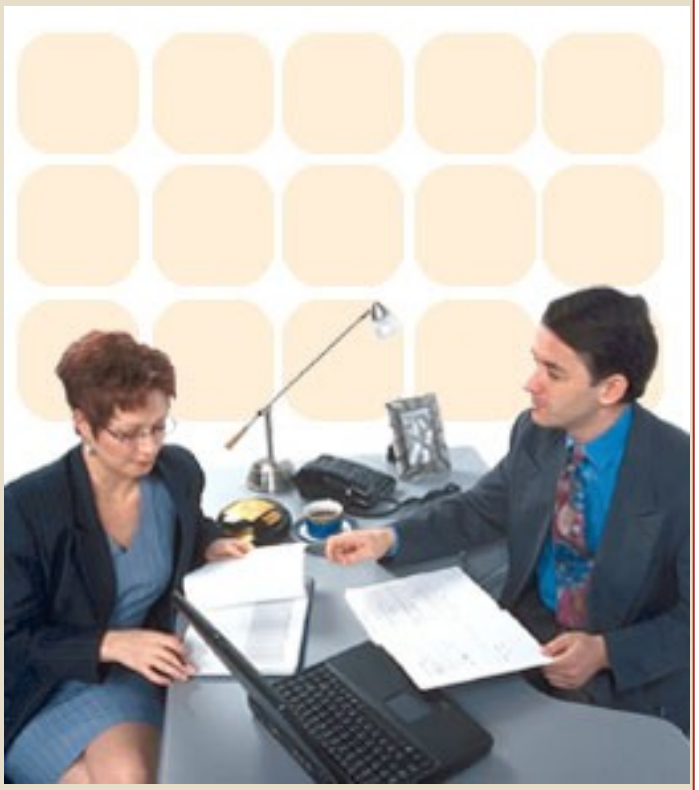


- The benefits of independence include:
  - Independent testers see different defects, and are unbiased.
  - An independent tester can verify assumptions people made during specification and implementation of the system.
- Drawbacks include:
  - Isolation from the development team
  - Independent testers may be the bottleneck as the last checkpoint.
  - Developers may lose a sense of responsibility for quality.

# Working as a test leader



- Test leader :
  - Plan, monitor, and control
  - Devise the test objectives, test policies, test strategies and test plans
  - Estimate the test and resources.
  - Plan for test automation if applicable.
  - Schedule, lead/guide, monitor, measure and evaluate its quality.
  - Ensure configuration management.
  - Report test progress, summary report.
  - Take action to compensate for problems.



# Working as a tester



- Tester:
  - Review and contribute to test plan.
  - Analyze, review and assess requirements/design specifications.
  - Create test specifications.
  - Setup test environment
  - Execute and log the tests, evaluate results and document problems found.
  - Automate tests.
  - Review tests developed by others.

# Defining the skills test staff need



- Application or business domain
- Technology
- Testing

# 5.2 Test planning and estimation (K2)



- Objectives
  - LO-5.2.1 Recognize the different levels and objectives of test planning. (K1)
  - LO-5.2.2 Summarize the purpose and content of the test plan, (IEEE 829). (K2)
  - LO-5.2.3 Differentiate between conceptually different test approaches(K2)
  - LO-5.2.4 Differentiate between the subject of test planning for a system and for scheduling test execution. (K2)

# 5.2 Test planning and estimation (K2)



- LO-5.2.5 Write a test execution schedule for a given set of test cases, considering prioritization, and technical and logical dependencies. (K3)
- LO-5.2.6 List test preparation and execution activities. (K1)
- LO-5.2.7 Factors that influence the effort related to testing. (K1)
- LO-5.2.8 Differentiate between the metrics based approach and the expert-based approach. (K2)
- LO-5.2.9 Recognize/justify adequate exit criteria for specific test levels. (K2)

# Introduction of planning



- Planning is required to achieve success.
- A plan describes a management approach, which, if followed, will ensure that the project achieves its objectives.


**Quality can be compromised if testing is not planned for and implemented.**

# What is project success?



- Project management activities should aim at ensuring that the project meets the following.
  - It is completed within the scheduled time.
  - It is completed within the budgeted cost.
  - It results in a good-quality product that fulfills customer requirements.

# Test planning (K2)



- Test Plan is a document describing the scope, approach, resources and schedule of intended test activities.

***Project management involves project planning, monitoring, and control to ensure project success.***

# IEEE 829 Standard Test Plan Template



- Test Plan Identifier
- Introduction
- Test Items
- Features to be tested
- Features not to be tested
- Approach
- Item pass/fail criteria
- Suspension and resumption criteria
- Test Deliverables
- Test Tasks
- Environmental needs
- Responsibilities
- Staffing and training needs
- Schedule
- Risks and contingencies
- Approvals

# Exit criteria (K2)



- The purpose of exit criteria is to define when to stop testing.
- Typically exit criteria may consist of:
  - Thoroughness measures, such as coverage of code, functionality or risk.
  - Estimates of defect density or reliability measures.
  - Cost.
  - Residual risks, such as defects not fixed or lack of test coverage in certain areas.
  - Schedules such as those based on time to market.

# Test estimation (K2)



- Two approaches for the estimation of test effort are covered in this syllabus:
  - The metrics-based approach: estimating the testing effort based on metrics of former or similar projects or based on typical values.
  - The expert-based approach: estimating the tasks by the owner of these tasks or by experts.

# Test estimation (K2)



- The testing effort may depend on a number of factors, including:
  - Characteristics of the product.
  - Characteristics of process
  - The outcome of testing: the number of defects and the amount of rework required.

# Test approaches (test strategies) (K2)

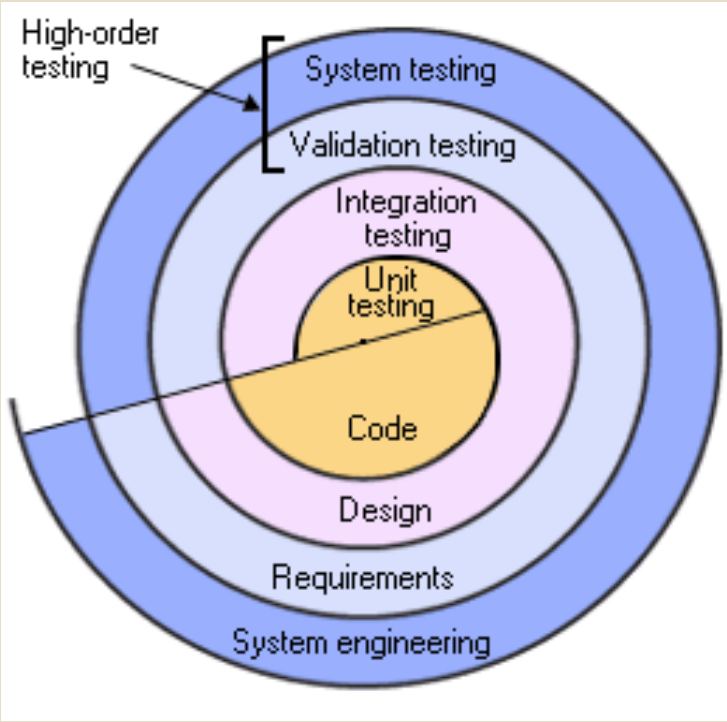


- One way to classify test approaches or strategies is based on the point in time at which the bulk of the test design work is begun:
  - Preventative approaches, where tests are designed as early as possible.
  - Reactive approaches, where test design comes after the software or system has been produced.

# Test approaches (test strategies) (K2)



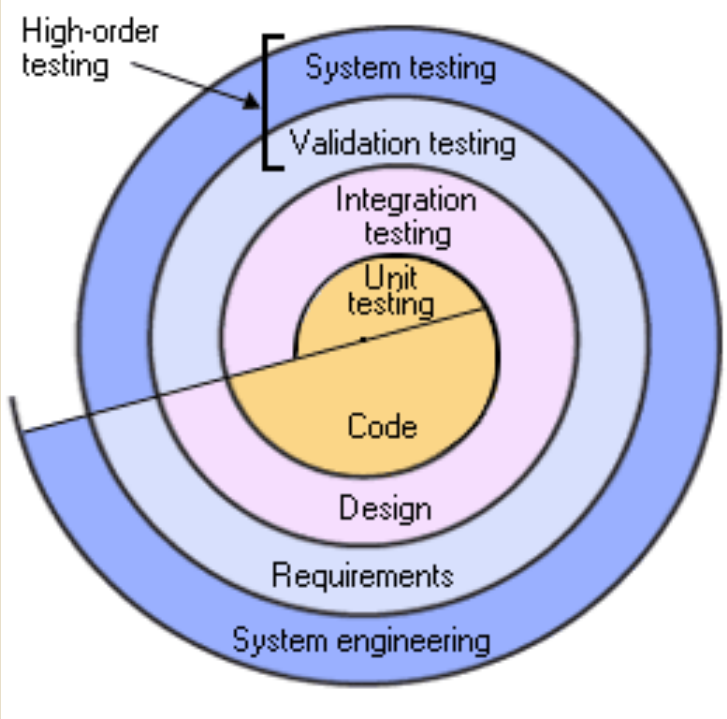
- Typical approaches or strategies include:
  - Analytical approaches:
    - Risk-based testing
  - Model-based approaches:
    - Stochastic testing using statistical information about failure rates.
  - Methodical approaches:
    - failure-based (error guessing and fault-attacks)



# Test approaches (test strategies) (K2)



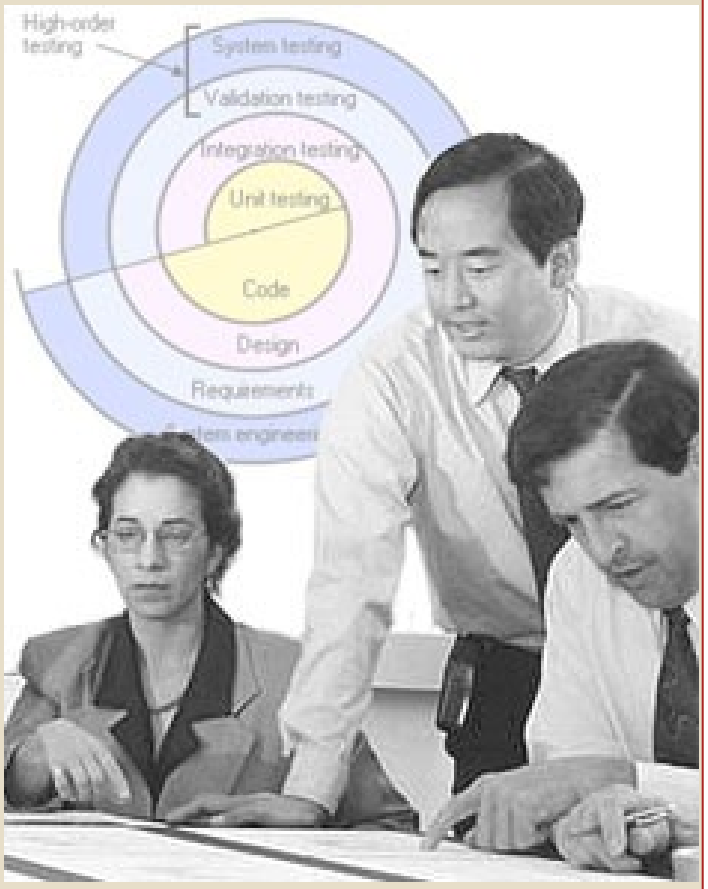
- Typical approaches or strategies include:
  - Process- or standard-compliant approaches.
    - Industrial specific standards
  - Dynamic and heuristic approaches.
    - Exploratory testing
  - Consultative approaches.
    - By advice and guidance of domain experts
  - Regression-averse approaches.
    - Reuse of existing material.



# Test approaches (test strategies) (K2)



- The selection of a test approach:
  - Risk of failure of the project, hazards to the product.
  - Skills and experience of the people, tools and methods.
  - The objective of the testing endeavor and the mission.
  - Regulatory aspects.
  - The nature of the product and the business.



# 5.3 Test progress monitoring and control



- Objectives
  - LO-5.3.1 Recall common metrics used for monitoring test preparation and execution. (K1)
  - LO-5.3.2 Understand and interpret test metrics for test reporting and test control (e.g. defects found and fixed, and tests passed and failed). (K2)
  - LO-5.3.3 Summarize the purpose and content of the test summary report document according to the 'Standard for Software Test Documentation' (IEEE 829). (K2)

# Monitoring the test activities

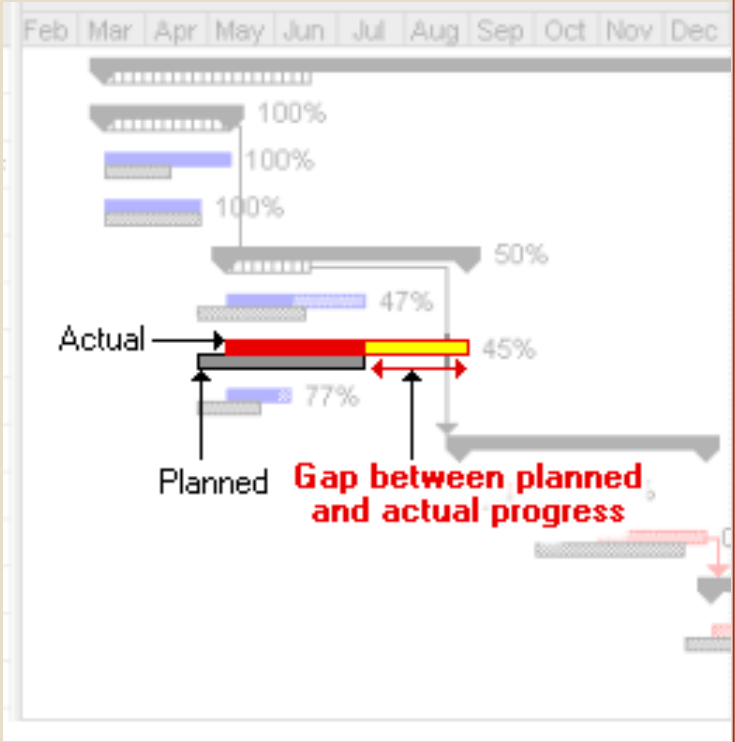


- Test monitoring:
  - Is a task of test management
  - Periodically checking the status of a test project
  - Report to compare the actual and planned
- Test Monitoring provides:
  - The feedback on how testing is going
  - Test results
  - The status of testing
  - Data for future test estimation

# Test progress monitoring



- Common test metrics include:
  - Percentage of work done in test case preparation.
  - Percentage of work done in test environment preparation.
  - Test case execution
  - Defect information
  - Test coverage.
  - Subjective confidence of testers in the product.
  - Dates of test milestones.
  - Testing costs.



# Test Summary Report



- Summary Report template IEEE 829
  - Test summary report identifier
  - Summary
  - Variances
  - Comprehensive assessment
  - Summary results
  - Evaluation
  - Summary of activities
  - Approval

# Test Summary Report



- **Test summary report identifier:**
  - A unique label so you can refer to that document.
- **Summary.**
  - Summarize what was tested and what happened. Point to all relevant documents.
- **Variances:**
  - If any test items differed from their specifications, the testing process didn't go as planned, why things were different.
- **Comprehensiveness assessment.**
  - How thorough was testing, in the light of how thorough the test plan said it should be? What wasn't tested well enough? Why not?

# Test Summary Report



- **Summary of results.**
  - Which problems have been dealt with? What problems remain?
- **Evaluation.**
  - How good are the test items? What's the risk that they might fail?
- **Summary of activities.**
  - In outline, what were the main things that happened? What did they cost (people, resource use, time, money)?
- **Approvals.**
  - Who has to approve this report? Get their signatures.

# Test control (K2)



- Test control describes any guiding or corrective actions.
- Examples of test control actions:
  - Making decisions based on information from test monitoring.
  - Re-prioritize tests.
  - Change the test schedule due to availability of a test environment.
  - Set an entry criterion.

# 5.4 Configuration management (K2)



- Objectives
  - LO-5.4.1 Summarize how configuration management supports testing. (K2)

# Configuration management



- Purpose:
  - All items of software are identified, version controlled, tracked for changes, related to each other and related to development items
  - All identified document and software items are referenced unambiguously in test document

# Configuration management



- **Configuration management:**
  - 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. [IEEE 610]
- **Configuration management tool:**
  - A tool that provides support for the identification and control of configuration items, their status over changes and versions, and the release of baselines consisting of configuration items.

# Configuration management



- Configuration control (version control)
  - An element of configuration management, consisting of the evaluation, co-ordination, approval or dis-approval and implementation of changes to configuration items after formal establishment of their configuration identification

# 5.5 Risk and testing (K2)



- Objectives
  - LO-5.5.1 Describe a risk as a possible problem that would threaten the achievement of one or
  - more stakeholders' project objectives. (K2)
  - LO-5.5.2 Remember that risks are determined by likelihood (of happening) and impact (harm
  - resulting if it does happen). (K1)
  - LO-5.5.3 Distinguish between the project and product risks. (K2)
  - LO-5.5.4 Recognize typical product and project risks. (K1)
  - LO-5.5.5 Describe, using examples, how risk analysis and risk management may be used for test
  - planning. (K2)

# Project risks (K2)



- Project risks are the risks that surround the project's capability to deliver its objectives, such as:
  - Logistics or product quality problem that block the tests
  - Excessive change to the product that invalidates test results
  - Insufficient or unrealistic test environments that yield misleading results

# Project risks (K2)



- Other Project risks
  - Organizational factors:
    - Skill and staff shortages;
    - Personal and training issues;
    - Political issues
    - Improper attitude toward or expectations of testing
  - Technical issues:
    - Problems in defining the right requirements;
    - The quality of the design, code and tests.
  - Supplier issues

# Product risks (K2)



- Product risks: Potential failure areas in the software or system such as:
  - Failure-prone software delivered.
  - The potential that the software/hardware could cause harm.
  - Poor software characteristics (e.g. functionality, reliability, usability and performance).
  - Software that does not perform its intended functions.

# Steps of the risk management model



- The five steps of the risk management model are given below:
  - Identifying risks
  - Analyzing risks
  - Planning for risks
  - Tracking risks
  - Controlling risks

# 5.6 Incident Management (K3)



- Objectives
  - LO-5.6.1 Recognize the content of an incident report according to the ‘Standard for Software
  - Test Documentation’ (IEEE 829). (K1)
  - LO-5.6.2 Write an incident report covering the observation of a failure during testing. (K3)

# Incident Management



- The objectives of testing is to find defects
- The discrepancies between actual and expected outcomes need to be logged as incidents.
- Incidents may be raised during development, review, testing or use of a software product.

# Incident Management



- Incident reports have the following objectives:
  - Provide developers and other parties with feedback about the problem to enable identification, isolation and correction as necessary.
  - Provide test leaders a means of tracking the quality of the system under test and the progress of the testing.
  - Provide ideas for test process improvement.

# IEEE 829 Standard: Test Incident Report Template



- Test incident identifier
- Summary
- Incident description
  - Input
  - Expected results
  - Actual results
  - Anomalies
  - Date and time
  - Procedure step
  - Environment
  - Attempts to repeat
  - Testers and observed
- Impact

# Incident Management



- Details of the incident report may include:
  - Date of issue, issuing organization, and author.
  - Expected and actual results.
  - Identification of the test item (configuration item) and environment.
  - Software or system life cycle process in which the incident was observed.
  - Description of the incident to enable reproduction and resolution, including logs, database dumps or screenshots.
  - Scope or degree of impact on stakeholder(s) interests.
  - Severity of the impact on the system.
  - Urgency/priority to fix.

# Incident Management



- Details of the incident report may include:
  - Status of the incident (e.g. open, deferred, duplicate, waiting to be fixed, fixed awaiting retest, closed).
  - Conclusions, recommendations and approvals.
  - Global issues, such as other areas that may be affected by a change resulting from the incident.
  - Change history, such as the sequence of actions taken by project team members with respect to he incident to isolate, repair, and confirm it as fixed.
  - References, including the identity of the test case specification that revealed the problem.

# References




- ISTQB Foundation Syllabus
- Foundation of Software Testing: ISTQB Certification
  - Dorothy Graham, Erik Van Veenedaal, Isabel Ivan, Rex Black
- Software Testing Practice: Test Management (Advance ISTQB)
  - Andreas Spillner, Thomas Rossner, Mario Winter, Tilo Linz
- IEEE Software Test Documentation, a summary
  - http://www.cs.otago.ac.nz/cosc345/lecs/lec22/testplan.htm

# Q & A

# Glossary



- **test policy:** A high level document describing the principles, approach and major objectives of the organization regarding testing.
- **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 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).

# Glossary



- **test plan:** 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 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.

# Glossary



- **test design specification:** A document specifying the test conditions (coverage items) for a test item, the detailed test approach and identifying the associated high level test cases.
- **test case specification:** A document specifying a set of test cases (objective, inputs, test actions, expected results, and execution preconditions) for a test item. [After IEEE 829]
- **test procedure specification:** A document specifying a sequence of actions for the execution of a test. Also known as test script or manual test script. [After IEEE 829]
- **test design technique:** Procedure used to derive and/or select test cases.

# Glossary



- **configuration control:** An element of configuration management, consisting of the evaluation, co-ordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification. [IEEE 610]
- **configuration management:** 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. [IEEE 610]

# Glossary



- **configuration management tool:** A tool that provides support for the identification and control of configuration items, their status over changes and versions, and the release of baselines consisting of configuration items.
- **test environment:** An environment containing hardware, instrumentation, simulators, software tools, and other support elements needed to conduct a test. [After IEEE 610]