Australian Government
Department of Defence

Defence Signals Directorate

Australasian Information Security Evaluation Program

Coverage (ATE_COV.3) - CC V2.2

Common Evaluation Methodology

21 December 2005

Version 1.1

Amendment Record

Version	Date	Description
1.0	12 December 2005	Released.
1.1	21 December 2005	Releasable to AISEFs

Table of Contents

1 Rigorous analysis of coverage (ATE_COV.3)

1.1 Objectives

1 The objectives of this sub-activity are to establish that the TSF has been tested against its functional specification in a systematic and exhaustive manner. This is to be achieved through an examination of developer analysis of correspondence.

1.2 Input

2 The evaluation evidence for this sub-activity is:

a) the ST;

b) the functional specification;

c) the test documentation;

d) the test coverage analysis.

1.3 Evaluator Actions

1.3.1 ATE_COV.3.1E

ATE_COV.3.1C	The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.3-1 The evaluator ***shall examine*** the test coverage analysis to determine that the correspondence between the tests identified in the test documentation and the functional specification is accurate.

3 Correspondence may take the form of a table or matrix. In some cases mapping may be sufficient to show test correspondence. In other cases a rationale (typically prose) may have to supplement the correspondence analysis provided by the developer.

4 Figure 1 displays a conceptual framework of the correspondence between security functions described in the functional specification and the tests outlined in the test documentation used to test them. Tests may involve one or multiple security functions depending on the test dependencies or the overall goal of the test being performed.

5 The identification of the tests and the security functions presented in the test coverage analysis has to be unambiguous. The test coverage analysis will allow the evaluator to trace the identified tests back to the test documentation and the particular security function being tested back to the functional specification.

ATE_COV.3-2 The evaluator ***shall examine*** the test documentation to determine that the testing approach for each security function of the TSF is suitable to demonstrate the expected behaviour.

6 Before the adequacy of test documentation can be accurately evaluated, or before new tests can be created, the evaluator has to understand the desired expected behaviour of a security function in the context of the requirements it is to satisfy.

7 The evaluator may choose to focus on one security function of the TSF at a time. For each security function, the evaluator reviews the ST requirement and the relevant parts of the functional specification, high-level design and guidance documentation to gain an understanding of the way the TOE is expected to behave.

8 With an understanding of the expected behaviour, the evaluator reviews the test documentation to gain an understanding of the testing approach. In most cases, the testing approach will entail a security function being stimulated at either the external or internal interfaces and its responses are observed. However, there may be cases where a security function cannot be adequately tested at an interface (as may be the case, for instance, for residual information protection functionality); in such cases, other means will need to be employed.

9 In cases where it is impractical or inadequate to test at an interface, the test documentation should identify the alternate approach to verify expected behaviour. It is the evaluator's responsibility to determine the suitability of the alternate approach. However, the following should be considered when assessing the suitability of alternate approaches:

a) an analysis of the implementation representation to determine that the required behaviour should be exhibited by the TOE is an acceptable alternate approach. This could mean a code inspection for a software TOE or perhaps a chip mask inspection for a hardware TOE.

b) it is acceptable to use evidence of developer integration or module testing, even if the EAL is not commensurate with evaluation exposure to the low-level design or implementation. If evidence of developer integration or module testing is used in verifying the expected behaviour of a security function, care should be given to confirm that the testing evidence reflects the current implementation of the TOE. If the subsystem or modules have been changed since testing occurred, evidence that the changes were tracked and addressed by analysis or further testing will usually be required.

10 It should be emphasized that supplementing the testing effort with alternate approaches should only be undertaken when both the developer and evaluator determine that there exists no other practical means to test the expected behaviour of a security function. This alternative is made available to the developer to minimize the cost (time and/or money) of testing under the circumstances described above; it is not designed to give the evaluator more latitude to demand unwarranted additional information about the TOE, nor to replace testing in general.

ATE_COV.3-3 The evaluator ***shall examine*** the test procedures to determine that the test prerequisites, test steps and expected result(s) adequately test each security function.

11 Test pre-requisites are necessary to establish the required initial conditions for the test. They may be expressed in terms of parameters that must be set or in terms of test ordering in cases where the completion of one test establishes the necessary pre-requisites for another test. The evaluator must determine that the pre-requisites are complete and appropriate in that they will not bias the observed test results towards the expected test results.

12 The test steps and expected results specify the actions and parameters to be applied to the interfaces as well as how the expected results should be verified and what they are. The evaluator must determine that the test steps and expected results are consistent with the functional specification and the high-level design. The tests must verify behaviour documented in these specifications. This means that each security functional behaviour characteristic explicitly described in the functional specification and high-level design should have tests and expected results to verify that behaviour.

13 For this sub-activity, exhaustive specification testing of the interfaces is required. The overall aim of this activity is to determine that each security function has been sufficiently tested against the behavioural claims in the functional specification and the design documentation. The test procedures will provide insight as to how the security functions have been exercised by the developer during testing. The evaluator will use this information when developing additional tests to independently test the TOE.

ATE_COV.3.2C	The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.3-4 The evaluator ***shall examine*** the test coverage analysis to determine that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

14 All security functions and interfaces that are described in the functional specification have to be present in the test coverage analysis and mapped to tests in order for completeness to be claimed. As Figure 1 displays, all the security functions have tests attributed to them and therefore complete test coverage is depicted in this example. Incomplete coverage would be evident if a security function was identified in the test coverage analysis and no tests could be attributed to it.

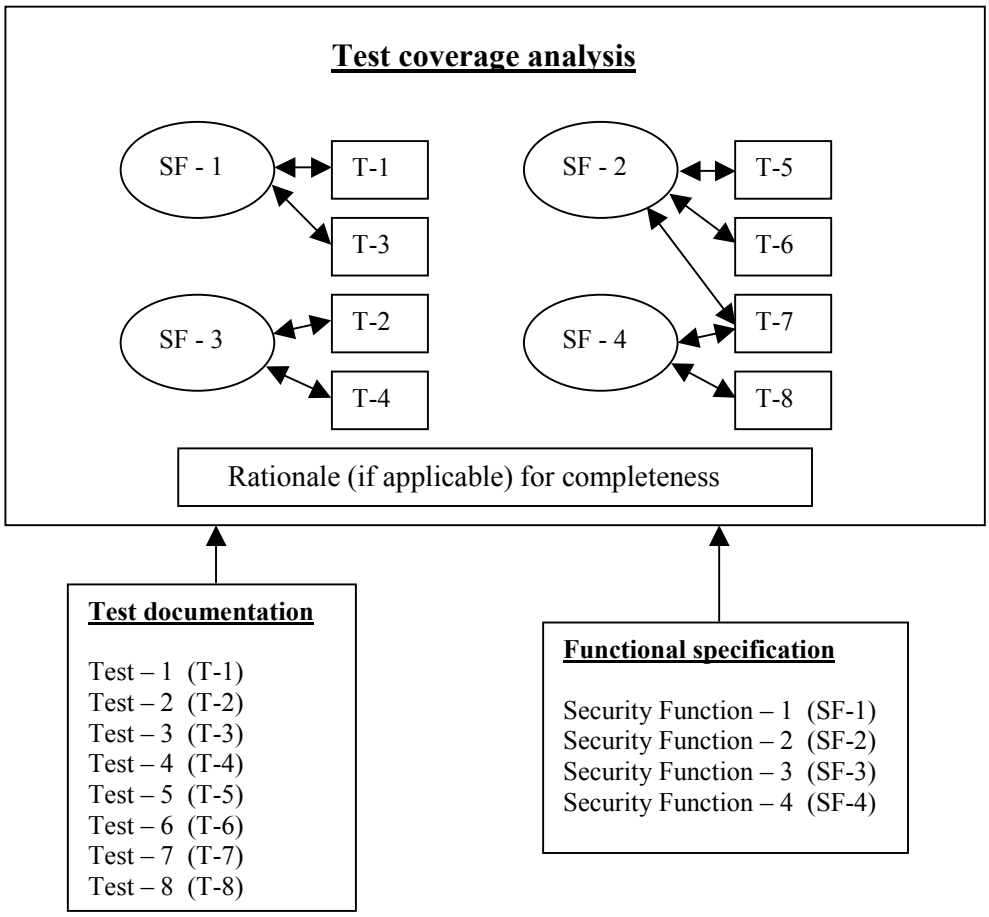

Figure 1: Conceptual Framework for Test Coverage

ATE_COV.3.3C	**The analysis of the test coverage shall rigorously demonstrate that all external interfaces of the TSF identified in the functional specification have been completely tested.**

ATE_COV.3-5 The evaluator ***shall examine*** the test coverage analysis to determine that the all external interfaces of the TSF identified in the functional specification have been completely tested.

15 For each TSFI in the functional specification to be completely tested, the developer's test coverage analysis must show that the set of tests:

a) Exercise all parameters including values in acceptable ranges, at the boundary of acceptable ranges and outside of acceptable ranges at each TSFI;

b) Exercise all exceptions that are observable at each TSFI;

c) Generate all the error messages that are observable at each TSFI; and

d) Demonstrate all effects observable at each TSFI.

16 The evaluator should use the functional specification to verify that the test coverage analysis is rigorous in that all parameters, effects, exceptions and error messages associated with the all TSFIs have been tested and that every TSFI in the functional specification has been completely tested. The evaluator should note that a suite of tests may be necessary in order to completely test a TSFI. The evaluator looks for errors or omissions in the test coverage analysis where the sum of the tests associated with a TSFI do not completely test the parameters, effects, exceptions and error messages that are associated with the TSFI as documented in the functional specification.