Australian Government
Department of Defence

Defence Signals Directorate

Australasian Information Security Evaluation Program

Independent testing (ATE_IND.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 Independent testing - complete (ATE_IND.3)

1.1 Objectives

1 The goal of this activity is to determine, by independently testing a subset of the TSF, whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing all of the developer's tests.

1.2 Input

2 The evaluation evidence for this sub-activity is:

a) the ST;

b) the functional specification;

c) the user guidance;

d) the administrator guidance;

e) the secure installation, generation, and start-up procedures;

f) the test documentation;

g) the test coverage analysis;

h) the depth of testing analysis;

i) the TOE suitable for testing.

1.3 Evaluator Actions

1.3.1 ATE_IND.3.1E

ATE_IND.3.1C	The TOE shall be suitable for testing.

ATE_IND.3-1 The evaluator ***shall examine*** the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.

3 The TOE used for evaluator testing should have the same unique reference as established by the CM capabilities (ACM_CAP).* sub-activity.

4 It is possible for the ST to specify more than one configuration for evaluation. The TOE may be composed of a number of distinct hardware and software implementations that need to be tested in accordance with the ST. The evaluator's TOE test configurations should be consistent with each evaluated configuration described in the ST.

5 The evaluator should consider the assumptions about the security aspects of the TOE environment described in the ST that may apply to the test environment. There may be some assumptions in the ST that do not apply to the test environment. For example, an assumption about user clearances may not apply; however, an assumption about a single point of connection to a network would apply.

6 If any test resources are used (e.g. meters, analysers) it will be the evaluator's responsibility to ensure that these resources are calibrated correctly.

ATE_IND.3-2 The evaluator ***shall examine*** the TOE to determine that it has been installed properly and is in a known state.

7 It is possible for the evaluator to determine the state of the TOE in a number of ways. For example, previous successful completion of the ADO_IGS.1 Installation, generation, and start-up procedures sub-activity will satisfy this work unit if the evaluator still has confidence that the TOE being used for testing was installed properly and is in a known state. If this is not the case, then the evaluator should follow the developer's procedures to install, generate and start up the TOE, using the supplied guidance only.

8 If the evaluator has to perform the installation procedures because the TOE is in an unknown state, this work unit when successfully completed could satisfy work unit ADO_IGS.1-2.

ATE_IND.3.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.3-3 The evaluator ***shall examine*** the set of resources provided by the developer to determine that they are equivalent to the set of resources used by the developer to functionally test the TSF.

9 The resource set may include laboratory access and special test equipment, among others. Resources that are not identical to those used by the developer need to be equivalent in terms of any impact they may have on test results.

1.3.2 ATE_IND.3.2E

ATE_IND.3.2E	The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.3-4 The evaluator ***shall devise*** a test subset.

10 The evaluator selects a test subset and testing strategy that is appropriate for the TOE. One extreme testing strategy would be to have the test subset contain as many security functions as possible tested with little rigour. Another testing strategy would be to have the test subset contain a few security functions based on their perceived relevance and rigorously test these functions.

11 Typically the testing approach taken by the evaluator should fall somewhere between these two extremes. The evaluator should exercise most of the security functional requirements identified in the ST using at least one test, but testing need not demonstrate exhaustive specification testing.

12 The evaluator, when selecting the subset of the TSF to be tested, should consider the following factors:

a) The developer test evidence. The developer test evidence consists of: the test coverage analysis, the depth of testing analysis, and the test documentation. The developer test evidence will provide insight as to how the security functions have been exercised by the developer during testing. The evaluator applies this information when developing new tests to independently test the TOE. Specifically the evaluator should consider:

   i) augmentation of developer testing for specific security function(s). The evaluator may wish to perform more of the same type of tests by varying parameters to more rigorously test the security function.

   ii) supplementation of developer testing strategy for specific security function(s). The evaluator may wish to vary the testing approach of a specific security function by testing it using another test strategy.

b) The number of security functions from which to draw upon for the test subset. Where the TOE includes only a small number of security functions, it may be practical to rigourously test all of the security functions. For TOEs with a large number of security functions this will not be cost-effective, and sampling is required.

c) Maintaining a balance of evaluation activities. The evaluator effort expended on the test activity should be commensurate with that expended on any other evaluation activity.

13 The evaluator selects the security functions to compose the subset. This selection will depend on a number of factors, and consideration of these factors may also influence the choice of test subset size:

a) Rigour of developer testing of the security functions. All security functions identified in the functional specification had to have developer test evidence attributed to them as required by ATE_COV.X sub-activity. Those security functions that the evaluator determines require additional testing should be included in the test subset.

b) Developer test results. If the results of developer tests cause the evaluator to doubt that a security function, or aspect thereof, operates as specified, then the evaluator should include such security functions in the test subset.

c) Known public domain weaknesses commonly associated with the type of TOE (e.g. operating system, firewall). Known public domain weaknesses associated with the type of TOE will influence the selection process of the test subset. The evaluator should include those security functions that address known public domain weaknesses for that type of TOE in the subset (know public domain weaknesses in this context does not refer to vulnerabilities as such but to inadequacies or problem areas that have been experienced with this particular type of TOE). If no such weaknesses are known, then a more general approach of selecting a broad range of security functions may be more appropriate.

d) Significance of security functions. Those security functions more significant than others in terms of the security objectives for the TOE should be included in the test subset.

e) SOF claims made in the ST. All security functions for which a specific SOF claim has been made should be included in the test subset.

f) Complexity of the security function. Complex security functions may require complex tests that impose onerous requirements on the developer or evaluator, which will not be conducive to cost-effective evaluations. Conversely, complex security functions are a likely area to find errors and are good candidates for the subset. The evaluator will need to strike a balance between these considerations.

g) Implicit testing. Testing some security functions may often implicitly test other security functions, and their inclusion in the subset may maximize the number of security functions tested (albeit implicitly). Certain interfaces will typically be used to provide a variety of security functionality, and will tend to be the target of an effective testing approach.

h) Types of interfaces to the TOE (e.g. programmatic, command-line, protocol). The evaluator should consider including tests for all different types of interfaces that the TOE supports.

i) Functions that are innovative or unusual. Where the TOE contains innovative or unusual security functions, which may feature strongly in marketing literature, these should be strong candidates for testing.

14 This guidance articulates factors to consider during the selection process of an appropriate test subset, but these are by no means exhaustive.

15 For guidance on sampling see B.2.

ATE_IND.3-5 The evaluator ***shall produce*** test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible.

16 With an understanding of the expected behaviour of a security function, from the ST and the functional specification, the evaluator has to determine the most feasible way to test the function. Specifically the evaluator considers:

a) the approach that will be used, for instance, whether the security function will be tested at an external interface, at an internal interface using a test harness, or will an alternate test approach be employed (e.g. in exceptional circumstances, a code inspection);

b) the security function interface(s) that will be used to stimulate the security function and observe responses;

c) the initial conditions that will need to exist for the test (i.e. any particular objects or subjects that will need to exist and security attributes they will need to have);

d) special test equipment that will be required to either stimulate a security function (e.g. packet generators) or make observations of a security function (e.g. network analysers).

17 The evaluator may find it practical to test each security function using a series of test cases, where each test case will test a very specific aspect of expected behaviour.

18 The evaluator's test documentation should specify the derivation of each test, tracing it back to the relevant design specification, and to the ST, if necessary.

ATE_IND.3-6 The evaluator ***shall conduct*** testing.

19 The evaluator uses the test documentation developed as a basis for executing tests on the TOE. The test documentation is used as a basis for testing but this does not preclude the evaluator from performing additional ad hoc tests. The evaluator may devise new tests based on behaviour of the TOE discovered during testing. These new tests are recorded in the test documentation.

ATE_IND.3-7 The evaluator ***shall record*** the following information about the tests that compose the test subset:

a) identification of the security function behaviour to be tested;
b) instructions to connect and setup all required test equipment as required to conduct the test;
c) instructions to establish all prerequisite test conditions;
d) instructions to stimulate the security function;
e) instructions for observing the behaviour of the security function;
f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;

g) instructions to conclude the test and establish the necessary post-test state for the TOE;

h) actual test results.

20 The level of detail should be such that another evaluator could repeat the tests and obtain an equivalent result. While some specific details of the test results may be different (e.g. time and date fields in an audit record) the overall result should be identical.

21 There may be instances when it is unnecessary to provide all the information presented in this work unit (e.g. the actual test results of a test may not require any analysis before a comparison between the expected results can be made). The determination to omit this information is left to the evaluator, as is the justification.

ATE_IND.3-8 The evaluator ***shall check*** that all actual test results are consistent with the expected test results.

22 Any differences in the actual and expected test results may indicate that the TOE does not perform as specified or that the evaluator test documentation may be incorrect. Unexpected actual results may require corrective maintenance to the TOE or test documentation and perhaps require rerunning of impacted tests and modifying the test sample size and composition. This determination is left to the evaluator, as is its justification.

1.3.3 ATE_IND.3.3E

ATE_IND.3.3E	The evaluator shall execute **all** tests in the test documentation to verify the developer test results.

ATE_IND.3-9 The evaluator ***shall conduct*** testing of all tests found in the developer test plan and procedures.

23 The overall aim of this work unit is to repeat all developer testing to confirm the validity of the developer's test results.

ATE_IND.3-10 The evaluator ***shall check*** that all the actual test results are consistent with the expected test results.

24 Inconsistencies between the developer's expected test results and actual test results will compel the evaluator to resolve the discrepancies. Inconsistencies encountered by the evaluator could be resolved by a valid explanation and resolution of the inconsistencies by the developer.

25 If a satisfactory explanation or resolution can not be reached, the evaluator's confidence in the developer's test results may be lessened. Ultimately, deficiencies with the developer's tests need to result in either corrective action to the developer's tests or in the production of new tests by the evaluator.

ATE_IND.3-11 The evaluator ***shall report*** in the ETR the evaluator testing effort, outlining the testing approach, configuration, depth and results.

26 The evaluator testing information reported in the ETR allows the evaluator to convey the overall testing approach and effort expended on the testing activity during the evaluation. The intent of providing this information is to give a meaningful overview of the testing effort. It is not intended that the information regarding testing in the ETR be an exact reproduction of specific test instructions or results of individual tests. The intention is to provide enough detail to allow other evaluators and overseers to gain some insight about the testing approach chosen, amount of evaluator testing performed, amount of developer tests performed, TOE test configurations, and the overall results of the testing activity.

27 Information that would typically be found in the ETR section regarding the evaluator testing effort is:

a) TOE test configurations. The particular configurations of the TOE that were tested.

b) subset size chosen for ATE_IND.3.2E. The amount of security functions that were tested during the evaluation and a justification for the size.

c) selection criteria for the security functions that compose the subset in ATE_IND.3.2E. Brief statements about the factors considered when selecting security functions for inclusion in the subset.

d) security functions tested. A brief listing of the security functions that merited inclusion in the subset ATE_IND.3.2E.

e) developer tests performed. The amount of developer tests performed (in this case all).

f) verdict for the activity. The overall judgement on the results of testing during the evaluation.

28 This list is by no means exhaustive and is only intended to provide some context as to the type of information that should be present in the ETR concerning the testing the evaluator performed during the evaluation.