



Specific Accreditation Criteria

ISO/IEC 17025 Application Document Manufactured Goods - Annex

**Software product and information system
testing**

XXXXXXXXXXXX 2025

© Copyright National Association of Testing Authorities, Australia 2013

This publication is protected by copyright under the Commonwealth of Australia Copyright Act 1968.

NATA's accredited facilities or facilities seeking accreditation may use or copy this publication or print or email this publication internally for accreditation purposes.

Individuals may store a copy of this publication for private non-commercial use or copy a reasonable portion of this publication in accordance with the fair dealing provisions in Part III Division 3 of the Copyright Act 1968.

You must include this copyright notice in its complete form if you make a copy of this publication.

Apart from these permitted uses, you must not modify, copy, reproduce, republish, frame, upload to a third party, store in a retrieval system, post, transmit or distribute this content in any way or any form or by any means without express written authority from NATA.

Table of Contents **to be updated at final version**

Terms and definitions used in this document	4
Confidentiality	5
Scope of Accreditation	6
4 General requirements	6
4.1 Impartiality	6
5 Structural requirements	6
6 Resource requirements	7
6.2 Personnel	7
6.3 Facilities and environmental conditions	7
6.4 Equipment	7
6.5 Metrological traceability	8
6.6 Externally provided products and services	8
7 Process requirements	8
7.2 Selection, verification and validation of methods	8
7.2.1 Selection and verification of methods	8
7.2.2 Validation of methods	9
7.3 Sampling	10
7.4 Handling of test or calibration items	10
7.5 Technical records	10
7.6 Evaluation of measurement uncertainty	11
7.8 Reporting of results	11
7.8.1 General	11
7.8.3 Specific requirements for test reports	11
7.8.7 Reporting opinions and interpretations	11
7.11 Control of data and information management	11
References	13
Amendment Table	15

Software product and information system testing

This document provides interpretative criteria and recommendations for the application of ISO/IEC 17025 for both applicant and accredited facilities conducting software product and information system testing.

Applicant and accredited facilities must comply with all relevant documents in the NATA Accreditation Criteria (NAC) package for Manufactured Goods (refer to *NATA Procedures for Accreditation*).

The clause numbers in this document follow those of ISO/IEC 17025, but since not all clauses require interpretation the numbering may not be consecutive.

Terms and definitions used in this document

The following terms and definitions are provided only to facilitate understanding of this document. These definitions describe terms which are defined or used in national and international standards (e.g., ISO/IEC 25000 and AS/NZS ISO/IEC/IEEE 29119.1).

Evaluation	A technical operation that consists of producing an assessment of one or more characteristics of a software product according to a specified procedure. In the context of this document, this refers to software testing.
Evaluator	Individual or organisation that performs an evaluation. Referred to as 'facility' in this document. A 'tester' of software will perform work for the facility.
Evaluation requester	The person or organisation that requests a test evaluation. Referred to as 'customer' in this document.
Evaluation requirements	Description of the objectives of the test evaluation, generally relating to the product's intended use and associated risks.
Evaluation specification	Description of the scope of the evaluation and the measurements to be performed on the product submitted for evaluation and its various components.
Means of testing (MOT)	Hardware and/or software, and the procedures for its use, including the executable test suite itself, used to carry out the testing required.
Reference implementation	An implementation of one or more standards or specifications, against which a means of testing and test tools for those standards or specifications are tested, for the purposes of validation of those means of testing and test tools. The term 'validated reference implementation' is used if the reference implementation has been shown to be derived faithfully from (i.e. to be 'traceable' back to) the relevant standard or specification.
Requester's requirements	An initial version of the evaluation requirements provided by the evaluation requester.

Software developer (Product developer)	An organisation that performs development activities during the software lifecycle process.
Software product (product under test) evaluation	Technical operation that consists of producing an assessment of one or more characteristics of a software product according to a specified procedure.
Test case	A set of inputs, execution preconditions, and expected outcomes developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement
Test environment	Facilities, hardware, software, firmware, procedures, and documentation intended for or used to perform testing of software
Test item	A work product that is an object of testing. Also called implementation or test object.
Test method	Specified technical procedure for performing a testing service including: <ul style="list-style-type: none"> the specification of all the individual test cases of a test suite; the test tools (both hardware and software) used to run those test cases and the way in which those test tools are used; the procedures used to select and run the test cases; the procedures used to analyse the observations and state the results.
Test software	Software used to carry out or assist in carrying out the testing required.
Test suite	A complete set of test cases that is necessary to achieve a testing objective.
Test tool	Hardware and/or software, excluding the test suite itself, used to carry out or assist in carrying out the testing required.
Test verdict	A statement of 'pass', 'fail' or 'inconclusive', specified in a test case, concerning conformance of the software under test with respect to that test case when it is executed.

Confidentiality

Accredited facilities, including applicants, who conduct activities under the Australian Information Security Evaluation Program (AISEP) should be aware that NATA will exchange information of the facility's accreditation with the Australian Signals Directorate (ASD) in support of a Memorandum of Understanding between NATA and ASD. Relevant ASD staff may also attend these assessments, either as Technical Assessors, where appropriate, or as observers.

Scope of Accreditation

For facilities issuing compliance results to a published conformity assessment standard such as a product testing standard, NATA scopes of accreditation will include the name or identification of the published standard used.

4 General requirements

4.1 Impartiality

4.1.3 The desirability of testing software during the development process is recognised. In these circumstances, the facility shall have procedures for ensuring its independence and that of its staff from the development process, and for identifying and controlling potential conflicts of interest.

5 Structural requirements

5.4 Testing may be carried out in the facility's permanent site, at sites away from its permanent site, or in associated temporary or mobile site. Further, testing may be performed by a tester who is remote to the test environment with access by a network (e.g., the internet).

Regardless of where testing may be performed, the customer may contribute to setting up and maintenance of the test environment.

The following is a conceptual model of the various testing models:

Remote tester (e.g. access by internet)	Tester has remote access to the test facility, which houses the test environment	Tester has remote access to the remote test environment
Tester present on-site	Testing done at the test facility	The tester is located at the remote test environment
	Testing at test facility	Testing outside test facility (e.g. at customer premises or in-situ)

The important aspect of the model is that it expresses two independent dimensions of testing 'remoteness':

- the testing may be performed at the test facility or remote to the test facility.
- the tester may be co-located with the test environment, or they may be located remote to the test environment with network access (e.g. by the internet).

When a tester is working remotely and/or testing is being performed remote to the facility, the facility shall ensure the remote location of the tester and/or test environment does not affect the correctness and reliability of the tests performed.

5.6 Personnel who release test results shall have authority over the testing activities, including, where necessary, the authority to reject results when they are considered to be inadequate.

6 Resource requirements

6.2 Personnel

6.2.3 Individuals who issue test results assume responsibility for the technical validity and accuracy of all information contained in test reports. They must have and demonstrate a sound knowledge of:

- the principles of the activities they perform or supervise;
- the standards or specifications used for testing;
- where remote testing is to be performed, the individuals should have a sound knowledge of all procedures that are unique to remote testing (e.g. control of a remote environment, security of data, storage of documents and records, and connecting to a test environment from a remote location);
- the NATA Accreditation Criteria.

6.3 Facilities and environmental conditions

6.3.1 The term 'environment' includes all hardware, software, data and network that make up the testing setup, regardless of location (i.e. whether at a facility, a remote test environment, or at a customer's premises).

6.3.2 Where a remote tester or remote testing is involved, the test documentation must describe how control is maintained over the total test environment.

In particular, the documentation must describe how a tester maintains control of a test environment hosted in whole or in part at a customer's premises. For example, the tester must be aware of any software upgrade such as a service pack made to a component of the test environment.

6.3.3 The facility shall ensure that any interference from other activities in the system does not invalidate the result of the specified tests. Examples of such activities are uncontrolled network activity during a performance test, virus scanners, obsolete versions of software, and backing up.

6.3.4 The test environment and the software under test shall be controlled and records kept.

The facility must demonstrate how access to the remote tester's environment is controlled and maintained.

6.3.5 Where a tester is remote, the laboratory must demonstrate how access to the remote tester's environment is controlled.

Where a remote test environment is used (e.g. at a customer's premises), the facility must demonstrate how control of access to the test environment is maintained.

6.4 Equipment

6.4.1 Equipment includes hardware, software, data and network that make up the test environment including the test tools.

6.4.4 Smoke testing may be one way of ensuring a test environment has been set up to meet the facility's specifications. Smoke testing is a quick preliminary test of a system that is done to give confidence that all the hardware, software, data & network components are in place and that the system is working to at least a basic level as a precursor to full testing.

Commercial off-the-shelf test tools must also be verified for their intended use.

6.4.13 Test tools should be identified by at least their name, supplier and version number.

Hardware shall be identified and recorded to the extent necessary for the tests being undertaken in order to achieve repeatability and reproducibility, and bearing in mind the risk of recall due to hardware errors or configuration changes. When the facility builds a machine or test kit, records must be maintained of each item of hardware and software significant to the tests undertaken.

6.5 Metrological traceability

6.5.1 There shall be an overall program of means of testing (MOT) validation and test tool validation and this shall be designed and operated to ensure, whenever applicable, that the results of test tool validation are traceable to international standards of test tool equivalence.

In the absence of such standards, appropriate national or international harmonisation agreements shall be used, wherever applicable, to check the reliability of test tool validation results.

6.5.3 For software or system conformance tests where metrological traceability to SI units is not possible or relevant, a comparison with a '*reference implementation*' may be required. A particular implementation may be used as a reference implementation only if its behaviour when tested by the relevant conformance test suite is repeatable, and if the coverage of the conformance test cases it is capable of exercising is impartial towards the range of implementations that may have to be tested by the conformance test suite.

When at least one suitable implementation becomes available for use as a reference implementation, then the relevant test tools shall be validated against it within a reasonable period.

6.6 Externally provided products and services

6.6.1 Commercially available test tool validation services, software testing tools, hardware, and such consumables as portable storage devices and media (e.g., USB flash drives) are regarded as services and supplies.

7 Process requirements

7.2 Selection, verification and validation of methods

7.2.1 Selection and verification of methods

7.2.1.2 Test methods may include test plans, test suites, test cases including relevant input data, evaluation procedures, and test design specifications.

7.2.1.5 Tool verification is the process of confirming that a means of testing or test tool will produce results that are consistent with the specifications of the relevant test suites, with any relevant standards and, if applicable, a previously verified version of the means of testing or test tool.

7.2.2 Validation of methods

7.2.2.1 In-house modifications to test tools must be validated.

The facility shall document the procedure(s) it uses to validate new versions of each test tool, including its traceability to the master copy and where relevant, the consistency with previous results.

Initial validation of a test tool shall be made by testing the test tool against a '*reference implementation*', where available, using all the test cases from the complete conformance test suite that are applicable to the reference implementation.

If there is no suitable reference implementation that could be used to validate a test tool, then the facility shall define and document the procedures that it uses to check the correct operation of the test tool, and provide evidence that these procedures are also applied whenever the test tool is modified.

When the test tool validation is made using a reference implementation, the facility shall fully document the expected results (i.e. previously obtained results) from using the full conformance test suite to test the nominated reference implementation.

Records of test tool validations and re-validations must include:

- reasons for the cases being run;
- date;
- environment information;
- a summary of the results obtained;
- details of any discrepancies from the expected results;
- list of known defects;
- indicate the traceability to international standard test suites or appropriate authoritative specifications.

This shall apply to both validations performed by the facility or by an external supplier.

When the test method requires test software to be installed on the system under test, the facility shall specify a set of confidence tests (possibly a subset of the conformance test suite) and specify the procedures to run them to check that the test software has been installed correctly. The facility shall also specify procedures to ensure that all test software mounted on a system under test is derived faithfully from an appropriate master version held by the facility.

Whenever any change is made to the test tool or testing environment, or whenever there is any doubt about the correct operation of the test tool, it shall be re-validated by testing against the reference implementation, using an appropriate subset of the conformity test suite where necessary.

Whenever any discrepancy is shown by the running of such a subset of the test suite or whenever any major change is made to the test tools or testing environment, then the test tools shall be validated against the reference implementation using the

complete conformance test suite before any further testing of customers' systems takes place.

If there are any discrepancies from expected results of validations or re-validations, then the relevant test cases or the test tool itself shall be suspended from use until the discrepancies have been resolved.

Commercial off-the-shelf test tools in general use within their designed application range may be considered as sufficiently validated until a suitable means of independent validation becomes available.

7.3 Sampling

7.3.1 Sampling includes test case selection. Examples of sampling may include:

- selection of test cases to test different conditions and combination of variables;
- selection of regression tests to re-run;
- selection of source code to review based on risk;
- randomness testing in gaming systems.

7.3.3 Sampling records for testing conducted must be maintained. Associated records shall include, but not be limited to, the following:

- test case selection;
- justification of the test case selection;
- test plan.

The basis for the selection of test cases (i.e. risk assessment) shall be recorded.

7.4 Handling of test or calibration items

7.4.1 The requirements of this clause apply specifically to the test items. It is recognised that interactions between the test item, the test tools and the test environment may result in modifications occurring to the test item as part of the normal installation or testing process. The intent is to prevent unintended changes from occurring and to ensure that an unmodified version of the test item is always available.

7.4.2 Additional labelling of equipment under test may not be necessary for hardware and software identified by a manufacturer's model type or number as well as a unique serial number and version number.

In the case of software, copies of the test item may be made and used for testing provided that the copies are traceable back to the original supplied test item and are controlled, e.g. by lodgement in a version control system.

7.5 Technical records

7.5.1 No records should be kept on a remote system, except temporarily, so that the facility's central repository remains the single point for all test records.

Test tools must be identified by at minimum: name, supplier, and version number.

Where test records and data are stored temporarily in remote systems, the remote tester shall ensure that they are stored in a way that security requirements of confidentiality, integrity, and availability of test records are preserved.

Security requirements should apply to both physical and electronic security of test records and data. Electronic security should apply to whatever computer media are employed.

Electronic security should ensure that access to records and data is controlled by the tester both for their viewing and use.

7.6 Evaluation of measurement uncertainty

7.6.1 For quantitative measurements, additional consideration shall be given to results derived by computational methods as opposed to calculation methods.

Calculation methods may produce a result taking into account an exhaustive and rigorous approach of all possible factors influencing the measurand (e.g. thorough calculation from first principles or summation of all unique events).

Computational methods may estimate the measurand, by the use of simulation, empirical data sampling, or from sources of random data (e.g. n empirical samples, simulation from n random numbers).

Note: For further information please refer to ILAC-G17, *ILAC Guidelines for Measurement Uncertainty in Testing*.

7.8 Reporting of results

7.8.1 General

7.8.1.2 The facility shall have unambiguous procedures for ensuring the repeatability, reproducibility, and objectivity of the analysis of results which require interpretation before they can be reported.

The facility shall have procedures for re-running of test cases. These shall include:

- objective criteria to decide when to re-run cases;
- the process for deciding the outcome (e.g. pass or fail) ensuring repeatability, reproducibility and objectivity.

7.8.3 Specific requirements for test reports

7.8.3.2 Test reports shall indicate the test suites used to perform the tests.

7.8.7 Reporting opinions and interpretations

Opinions may be included in reports to:

- clarify the understanding of a test result;
- if applicable, provide advice on possible future directions of testing; and,
- fulfil customer requirements.

7.11 Control of data and information management

7.11.1 Any remote storage of records and documentation shall be temporary (e.g. a remote tester revising documentation).

7.11.3 The procedures to control computerised systems should address appropriate implementation of management and control configuration, maintenance of

traceability between related documents, and where appropriate a combination of manual and computer-based approaches.

7.11.5 The tester, when working remotely, shall have access to all necessary documentation.

DRAFT

References

This section lists publications referenced in this document and other useful references. The year of publication is not included as it is expected that only current versions of the references shall be used.

Standards

ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories*

Software evaluation standards

ISO/IEC 25000 *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE*

ISO/IEC 25010 *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*

ISO/IEC 25040 *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process*

ISO/IEC 25041 *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation guide for developers, acquirers and independent evaluators*

ISO/IEC 25045 *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation module for recoverability*

ISO/IEC 25051 *Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing*

Software testing standards

ISO/IEC/IEEE 29119-1 *Software and systems engineering — Software testing — Part 1: Concepts and definitions*

ISO/IEC/IEEE 29119-2 *Software and systems engineering — Software testing — Part 2: Test processes*

ISO/IEC/IEEE 29119-3 *Software and systems engineering — Software testing — Part 3: Test documentation*

Process assessment standards

ISO/IEC 33001	<i>Information technology — Process assessment — Concepts and terminology</i>
ISO/IEC 33002	<i>Information technology — Process assessment — Requirements for performing process assessment</i>
ISO/IEC 33003	<i>Information technology — Process assessment — Requirements for process measurement frameworks</i>
ISO/IEC 33004	<i>Information technology — Process assessment — Requirements for process reference, process assessment and maturity models</i>

Security techniques (Common Criteria) standards

ISO/IEC 15408-1	<i>Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model</i>
ISO/IEC 15408-2	<i>Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components</i>
ISO/IEC 15408-3	<i>Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components</i>
ISO/IEC 15408-4	<i>Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities</i>
ISO/IEC 15408-5	<i>Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements</i>
ISO/IEC 18045	<i>Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation</i>

NATA publications

NATA Accreditation Criteria (NAC) package for Manufactured Goods

ILAC publications

ILAC-G17 *ILAC Guidelines for Measurement Uncertainty in Testing*

Amendment Table

The table below provides a summary of changes made to the document with this issue.

Section or Clause	Amendment
Whole document	Minor editorial amendments. Redundant requirements that have been superseded by the current NATA Accreditation Criteria have been removed.
Title	The previous title of this document was <i>Specific Accreditation Criteria: ISO/IEC 17025 Application Document, Manufactured Goods - Annex, Software and information system performance testing</i> . The title has been changed because the testing activities covered by this document are not limited to performance testing.
7.3.3	Additional requirement for facilities to record the basis of their selection of test cases.
7.11.1	Remote storage of records shall be temporary only.