SKIM AKREDITASI MAKMAL MALAYSIA (SAMM)
LABORATORY ACCREDITATION SCHEME OF MALAYSIA

STR 1.13 - SPECIFIC TECHNICAL REQUIREMENTS FOR ACCREDITATION OF SOFTWARE TESTING LABORATORIES

Issue 2, 10 February 2022

(Supplementary to MS ISO/IEC 17025)

MS ISO/IEC 17025

JABATAN STANDARD MALAYSIA
Department of Standards Malaysia

TABLE OF CONTENTS

Introduction

This document describes requirements designed to apply to all types of testing objective and therefore need to be interpreted with respect to the type of testing concerned and the techniques involved.

This document does not re-state all the provisions of MS ISO/IEC 17025 and laboratories are reminded of the need to comply with all the relevant requirements detailed in MS ISO/IEC 17025. Laboratory is also reminded of the need to comply with any relevant statutory or legislative requirements.

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

This document shall be used by Department of Standards Malaysia (Standards Malaysia) to provide appropriate criteria for the assessment and accreditation of laboratories providing software testing services.

1 Scope

This document shall be read in conjunction with MS ISO/IEC 17025, SAMM Policy documents (SP series) and relevant requirements published by Standards Malaysia.

The scope of this document confines to requirements of conducting software testing for the purpose of laboratory accreditation.

The software categories in this scope of testing as prescribed in **Appendix 1** include but not limited to:

a) Security - Hardware (HD) Appliance Software (SW)
b) Security - Software
c) Hardware Appliances Software
d) Business (Groupware) Software
e) Embedded Software
f) Networking and Application Software
g) Big Data Analytics Software
h) Software other than malware and/or gambling software

The classes of test in this document include but not limited to the following tests:

a) System/Software Quality

    i) Functional Suitability
    ii) Reliability
    iii) Usability
    iv) Performance Efficiency
    v) Maintainability
    vi) Portability
    vii) Compatibility
    viii) Security

b) Data Quality

i) Accuracy
ii) Completeness
iii) Consistency
iv) Credibility
v) Currentness
vi) Accessibility
vii) Compliance
viii) Confidentiality
ix) Efficiency
x) Precision
xi) Traceability
xii) Understandability
xiii) Availability
xiv) Portability
xv) Recoverability

2 Normative references

This document refers to the following standards and the latest editions of the referenced documents (including any amendments) apply: -

i) MS ISO/IEC 17025 - General Requirements for the Competence of Testing and Calibration Laboratories

ii) SAMM Policy Documents

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

iv) ISO/IEC 25012 - Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Data quality model

v) ISO/IEC 25023 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Measurement of system and software product quality

vi) ISO/IEC 25040 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Evaluation process

vii) ISO/IEC/IEEE 29119 - Software and systems engineering - Software testing

viii) Open Web Application Security Project (OWASP), OWASP Foundation Inc.

ix) MS ISO/IEC 15408-2 - Information technology -- Security techniques -- Evaluation criteria for IT security Part 2 - Security functional Components

x) Independent Verification and Validation (IV&V) Handbook, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU).

xi) Network Equipment Security Assurance Scheme (NESAS) Security Assurance Specifications (SCAS).

3 Terms and definitions

For the purposes of this document, the relevant terms and definitions below apply;

3.1 Commercial Off-The-Shelf (COTS)

Software product defined by a market-driven need, commercially available, and whose fitness for use has been demonstrated by a broad spectrum of commercial users.

3.2 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.

3.3 Malware software

Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also Spyware, programming that gathers information about a computer user without permission.

3.4 Measurement

A set of operations having the object of determining a value of a measure.

3.5 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.

3.6 Ready to Use Software Product (RUSP)

Software product available for any user, at cost or not, and use without the need to conduct development activities.

3.7 Software

All or part of the programs, procedures, rules and associated documentation of an information processing system.

3.8 Software product

The set of computer programs, procedures and possibly associated documentation and data.

3.9 Testing

The process of operating a system or component under specified conditions, observing or recording the results, and the process of analysing a software item to detect the differences between existing and required conditions (that is, bugs), and to evaluate the features of the software item.

3.10 Test case

A set of inputs, execution conditions, and expected results developed for a particular objective, such as exercise a particular program path or to verify compliance with a specific requirement.

3.11 Test suite

A set of test scripts or test procedures to be executed in a specific test run.

3.12 Test specification

A document that specifies the test inputs, execution conditions and predicts results for an item to be tested.

3.13 Test tool

Software or hardware that supports one or more test activities.

3.14 Validation

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

For other terms not defined in this document, the relevant terms and definitions given in ISO/IEC 25000 series and ISO/IEC 17000 apply.

4 General requirements

Same as in MS ISO/IEC 17025.

5 Structural requirements

Same as in MS ISO/IEC 17025.

6 Resource requirements

6.1 General

6.1.1 The laboratory shall have available the personnel, facilities, equipment, systems and support services necessary to manage and perform its laboratory activities.

Note: Where the laboratory is part of an organisation, support services refer to services obtained from providers outside the organisation as well as services obtained from other division / department within the organisation.

6.2 Personnel

The testing laboratory shall have sufficient personnel having appropriate technical competency to carry out the testing as prescribed in **Appendix 2** (Personnel Competency Table).

6.3 Facilities and environmental conditions

6.3.1 The word “environment” refers to hardware and associated software, including the required network connection on which the software being tested is running. The laboratory shall ensure that any interference from other activities in the system does not invalidate the result of the specified test.

6.3.2 Procedure to control handling of testing performed in an environment controlled by customer, developer or user shall be in place.

6.3.3 The test environment and the software being tested shall be appropriately monitored, controlled and recorded to ensure correct and complete identification at any time.

6.3.4 Access to facilities, network, operating systems, application and information related to the testing laboratory activities that may affect the outcome of the testing shall be appropriately controlled from unauthorized personnel.

6.3.5 There shall be effective separation of the testing environment including test tool, network connection and test items to ensure non-interference for each project.

6.4 Equipment

6.4.1 Equipment used for testing shall include hardware and software including the test tools that are not subjected to calibration.

6.5 Metrological traceability

6.5.1 In software testing, metrological traceability may be established through agreed methods or approach or consensus standards for software test tools by all parties concerned.

6.5.2 Calibration is not applicable for software test tools but software test tools used for testing need to be validated before use. However, any measuring equipment used to support the testing of this software where the measurement parameters of which have a significant effect on the validity of the result of the testing shall be calibrated with traceability to national or international standard.

6.6 Externally provided products and services

6.6.1 The laboratory shall use suitable products and, where possible, services of an accredited laboratory by Standards Malaysia or laboratory accredited by a signatory to a Mutual Recognition Arrangement such as Asia Pacific Accreditation Cooperation (APAC) and International Laboratory Accreditation Cooperation (ILAC). Where the externally services provider is not accredited, the laboratory shall evaluate and provide evidence of compliance with the relevant requirements of MS ISO/IEC 17025.

Products can include:
a) test tools,
b) hardware,
c) laptop and servers,
d) consumables such as CDs, and
e) external hard drives.

Services can include:
a) testing,
b) calibration,
c) proficiency testing, and
d) auditing.

6.6.2 For external testing services provider, the laboratory shall ensure that the external services provider's personnel possess suitable technical competency not less than those stated in **Appendix 2.**

7 Process requirements

7.1 Review of requests, tenders and contracts

7.1.1 Testing work shall be defined in Test Plans, Test Specifications, Test Cases, or other test suite deliverables as defined in the Test Methods. These can also be encompassed in an overall Test Plan with matching Test Report as defined by the methodology.

7.1.2 The test plans or test methods shall be reviewed and mutually agreed upon between customer and laboratory prior to execution.

7.1.3 Where relevant, the following shall be defined:

a) Criteria for running partial testing or re-testing test items; and
b) Decision rules on test anomaly characterisation such as severity or likelihood or priority.

7.2 Selection, verification and validation of methods

7.2.1 Selection and verification of methods

The test methods shall address but not limited to the following topics:

a) Test preparation and setup;

b) Test Item configuration management including versioning or releases of the test items;

c) Test coverage and traceability to requirements or standards;

d) Test case shall be clearly stated and documented having identified objective and traceability to requirements or standards and expected outcomes so as to avoid ambiguous results;

e) Automated test suites (if used) shall be traceable to the execution of the related test cases;

f) Test plan document shall be approved prior to testing;

g) Completed test cases shall be reviewed and approved prior to testing; and

h) Procedures for reporting anomaly severity classifications shall be defined.

7.2.2 Validation of methods

7.2.2.1 Testing tool shall be verified of its ability for reproducible and repeatable 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.

7.2.2.2 In-house modifications to test tools shall be validated. Initial validation of a test tool shall be made by testing the test tool against a ‘reference implementation’, using all the test cases from the complete conformance test suite that are applicable to the reference implementation.

7.2.2.3 A ‘reference implementation’, where available, shall be used for test tool validation. If there is no suitable ‘reference implementation’, then the laboratory shall define procedures that it uses to check the correct operation of the test tool. Records of test tool validations shall include reasons for the cases being run, date, environmental information (if appropriate), a summary of the results obtained, details of any discrepancies from the expected results and indicate the traceability to one of the following:

a) the test suites;

b) or appropriate authoritative specifications (such as OWASP, industry de facto standards etc.); and

c) where applicable, to international standards (such as ISO/IEC 25022 etc.).

7.2.2.4 This shall apply to both validations performed by the laboratory or by an external supplier. When the test method requires test software to be installed on the system under test, the laboratory shall check that the software has been installed correctly. 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'. Commercial off-the shelf test tools in general use within their designed application range may be considered as sufficiently verified until a suitable means of independent validation becomes available.

7.3 Sampling

7.3.1 Within the context of software testing, sampling may refer to test case selection which include:

a) selection of test cases to different conditions and combination variables; and

b) selection of regression tests to run.

7.3.2 Sampling records for testing conducted shall be maintained which may include:

a) Test plan;

b) Test cases and test data selection; and

c) Justification of the selection as in test plan.

7.4 Handling of test items

7.4.1 The interactions between the test items, the test tools and the test environment may result in modification to the software being tested as part of the normal installation or testing process. The laboratory shall protect products under test and verified tools used for the testing from any modification, unintended use or unauthorised access.

7.4.2 For evaluated product which include software component, the laboratory shall ensure that the configuration management mechanisms are in place to prevent unintended modifications to the software components during the testing process. Procedure to ensure proper retention, disposal or return of software and hardware after the completion of the testing shall be established and maintained.

7.5 Technical records

Same as in MS ISO/IEC 17025.

7.6 Evaluation of measurement uncertainty

7.6.1 For testing in qualitative nature, evaluation of measurement uncertainty is not applicable. For quantitative testing, where appropriate, measurement uncertainty shall be evaluated.

7.7 Ensuring the validity of results

Same as in MS ISO/IEC 17025 and SAMM Policy 4 (SP4) - Policy for Participation in Proficiency Testing Activities.

7.8 Reporting of results

Same as in MS ISO/IEC 17025.

7.9 Complaints

Same as in MS ISO/IEC 17025.

7.10 Nonconforming work

Control of non-conforming test refers to the results associated with nonconformance to the documented test methodologies and do not constitute to the non-conformities detected in the software being tested.

7.11 Control of data and information management

Same as in MS ISO/IEC 17025.

8 Management system requirements

8.1 Options

Same as in MS ISO/IEC 17025.

8.2 Management system documentation

Same as in MS ISO/IEC 17025.

8.3 Control of management system documents

8.3.1 Documents may include test plans, test suites and test cases. This should include relevant inputs, testing procedures and test design specification which shall be controlled, reviewed, approved and revised. Document may be suitably classified based on laboratory's identified classification levels (e.g. Top Secret, Secret, Confidential, Restricted and Public) and shall be managed, transferred, stored and disposed in accordance with the procedure appropriate to their classification.

8.4 Control of records

8.4.1 Records may be suitably classified based on laboratory's identified classification levels (e.g. Top Secret, Secret, Confidential, Restricted or Public) and should be managed, transferred, stored and disposed in accordance with the procedure appropriate to their classification. Laboratories shall have appropriate controls and procedures in place for the collection, storage,

manipulation, reduction and transmission of electronic data and results based on their classification level.

8.5 Actions to address risks and opportunities

Same as in MS ISO/IEC 17025.

8.6 Improvement

Same as in MS ISO/IEC 17025.

8.7 Corrective actions

Same as in MS ISO/IEC 17025.

8.8 Internal audits

Same as in MS ISO/IEC 17025.

8.9 Management reviews

Same as in MS ISO/IEC 17025.

Appendix 1

SCOPE OF ACCREDITATION / CERTIFICATION BASED ON CATEGORY CODES

1.	**Security-Hardware (HD) Appliance Software (SW)**	
	1.1	Hardware Appliance – Software product which is sold (provided) with Hardware
	1.2	Security – Software which is developed for information security (e.g. Intrusion Prevention System (IPS))
	1.3	Software product which is developed for Security and sold (provided) as a Hardware Appliance
2.	**Security**	
	2.1	Software product which is developed for Security not as a Hardware Appliance (e.g. Firewall, Antivirus, Anti-Spam, Spy web)
3.	**Hardware Appliance Software**	
	3.1	Software product which is developed generally for selling (providing) as a Hardware Appliance, not for Security (e.g. Smart card reader, mobile devices)
4.	**Business (Groupware) Software**	
	4.1	Software product which is developed for business use or office management of general company, so that every member of organization uses in office (e.g. draft, electronic approval, documentation disseminate, bulletin board, documentation management)
5.	**Embedded Software**	
	5.1	Software product which is performing specific function and is sold (provided) as a one-chip type embedded in Hardware parts without the third-party operating system (e.g. Software embedded in refrigerator, washing machine, printer)
	5.2	Software product which is embedded in Hardware, so that it cannot be accessed for modification/deletion in any way (e.g. software burning into chip, Read Only Memory (ROM))
6.	**Networking and Application Software**	
	6.1	Any networking device enables the user to access infrastructures such as IT/internet/finance/telecommunication/utility.
7.	**Big Data Analytics Software**	
	7.1	Software that has ability to analyse, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software.
8.	**Software other than malware and/or gambling software.**	
	8.1	Other Software not included in categories no. 1 to 7 above e.g. COTS/RUSP and customized software (MS Customer Relationship Management (CRM), LOB applications).
	8.1.1	Custom COTS Software
	8.1.2	Custom software (non COTS)

Appendix 2

PERSONNEL COMPETENCY TABLE

	Academic	Work Experience	Knowledge/Training/ Certification	Demonstrable Skills
Testers	Any tertiary education (degree) in any field of Information, Communication and Technology (ICT) or equivalent (technical field)	At least 1 year working experience with a minimum of 6 months experience in software testing	Knowledge of MS ISO/IEC 17025 Basic awareness of other standards or bodies of knowledge related to software testing domains or tools Professional Certification from Internationally Recognized Software Testing Body of Knowledge or relevant ICT Certification Body	Good understanding of the full test cycle which covers Test Planning, Test Analysis and Design, Environment Set Up, Test Execution and Reporting Able to conduct test analysis & design, and test execution for the relevant standards in use quality aspects to be tested
	Any tertiary education (diploma) in any field of ICT or equivalent (technical field)	At least 3 years working experience with a minimum of 6 months experience in software testing	Knowledge of MS ISO/IEC 17025 Basic awareness of other standards or bodies of knowledge related to software testing domains or tools Professional Certification from Internationally Recognized Software Testing Body of Knowledge or relevant ICT Certification Body	Good understanding of the full test cycle which covers Test Planning, Test Analysis and Design, Environment Set Up, Test Execution and Reporting Able to conduct test analysis & design, and test execution for the relevant standards in use quality aspects to be tested

	Academic	Work Experience	Knowledge/Training/ Certification	Demonstrable Skills
Approved Signatories	Any tertiary education (degree) in any field of Information, Communication and Technology (ICT) or equivalent (technical field)	At least 5 years working experience in relevant field with a minimum of 3 years experience in software testing	Knowledge of MS ISO/IEC 17025 Basic awareness of other standards or bodies of knowledge related to software testing domains or tools Professional Certification from Internationally Recognized Software Testing Body of Knowledge or relevant ICT Certification Body	Able to put into practice or confirm cycle which covers Test Planning, Test Analysis and Design, Environment Set Up, Test Execution and Reporting Able to conduct test analysis & design, and test execution for the relevant standard in use quality aspects to be tested Good understanding of software development and test lifecycle Able to conclude software quality conformance to standard in use of test being conducted
	Any tertiary education (diploma) in any field of ICT or equivalent (technical field)	At least 5 years working experience with a minimum of 3 years experience in software testing	Knowledge of MS ISO/IEC 17025 Basic awareness of other standards or bodies of knowledge related to software testing domains or tools. Professional Certification from Internationally Recognized Software Testing Body of Knowledge or relevant ICT Certification Body	Able to put into practice or confirm cycle which covers Test Planning, Test Analysis and Design, Environment Set Up, Test Execution and Reporting Able to conduct test analysis & design, and test execution for the relevant standard in use quality aspects to be tested Good understanding of software development and test lifecycle Able to conclude software quality conformance to standard in use of test being conducted

Bibliography

1. ISO/IEC 25041 - Systems and software engineering - Systems and Software Quality Requirements and Evaluation (SQuaRE) - Evaluation Guide for Developers, Acquirers and Independent Evaluators.

2. ISO/IEC/IEEE 29119-1 - Software and Systems Engineering - Software Testing.

3. 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.

4. IEEE 828-2012 - IEEE Standard for Configuration Management in Systems and Software Engineering.

5. ISO/IEC/IEEE 15939 - Systems and Software Engineering - Measurement Process.

6. ISO/IEC TR 13233 - Information Technology - Interpretation of Accreditation Requirements in ISO/IEC Guide 25 - Accreditation of Information Technology and Telecommunications Testing Laboratories for Software and Protocol Testing Services.

7. IEEE 829 - IEEE Standard for Software and System Test Documentation.

8. ISO/IEC 25022 - Systems And Software Engineering - Systems And Software Quality Requirements And Evaluation (SQuaRE) - Measurement of Quality In Use.

9. International Software Testing Qualifications Board (ISTQB) Glossary.

Acknowledgements

1.	Mr. Pua Hiang (Chairman)	Department of Standards Malaysia
2.	Ms. Siti Raikhan Aina Bogal (Secretariat)	Department of Standards Malaysia
3.	Mr. Hasiady Yasin	Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)
4.	Ms. Myzatul Akmam Sapaat	Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)
5.	Mr. Nashiruddin Mohd Tahir	Malaysia Industry - Government Group for High Technology (MIGHT)
6.	Ms. Norahana Salimin	Cybersecurity Malaysia
7.	Ms. Siti Fatimah Abidin	Cybersecurity Malaysia
8.	Mr. Mohd Khaizul Azhar Mohd Yusof	Malaysian Software Testing Board (MSTB)
9.	Ms. Pang Chia Chia	Malaysian Software Testing Board (MSTB)
10.	Ms. Anjana Devi N. Kuppusamy	MIMOS Berhad
11.	Mr. Ashok Sivaji	MIMOS Berhad
12.	Mr. Shahjerome Ambrose	AI Ain IT Consultants Sdn Bhd
13.	Mr. Saiful Adli Ismail	UTM Kuala Lumpur