NABL 137

National Accreditation Board for Testing and Calibration Laboratories (NABL)

SPECIFIC CRITERIA FOR ACCREDITATION OF SOFTWARE & IT SYSTEM TESTING LABORATORIES

ISSUE NO.: 01
ISSUE DATE: 14-Oct-2019

AMENDMENT NO.: --
AMENDMENT DATE: --

AMENDMENT SHEET

Sl	Page No.	Clause No.	Date of Amendment	Amendment	Reasons	Signature QM	Signature CEO
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

CONTENTS

ABBREVIATIONS

APAC	-	Asia Pacific Accreditation Cooperation
CAB	-	Conformity Assessment Body
CCCS	-	Common Control Criteria Standard
CIS	-	Centre for Internet Security
CWE	-	Common Weakness Enumeration
FRS	-	Functional Requirements Selection
GIGW	-	Guidelines for Indian Government Websites
IAAS	-	Infrastructure as a service
IEC	-	International Electro technical Commission
IEEE	-	Institute of Electrical and Electronics Engineers
ILAC	-	International Laboratory Accreditation Cooperation
IP	-	Internet Protocol
ISO	-	International Organization for Standardization
IT	-	Information Technology
H/W	-	Hardware
HTTPS	-	Hypertext Transfer Protocol Secure
MPLS	-	Multiprotocol Label Switching
MU	-	Measurement Uncertainty
NABL	-	National Accreditation Board for Testing and Calibration Laboratories
NIST	-	National Institute of Standards and Technology
OWASP	-	Open Web Application Security Project
PAAS	-	Platform as a service
RFP	-	Request for Proposal
RUSP	-	Requirements for quality of Ready to Use Software Product
S/W	-	Software
SOP	-	Standard Operating Procedure
SQuaRE	-	Systems and Software Quality Requirements and Evaluation
SRS	-	Software Requirements Selection
SUT	-	Software under Testing
TM	-	Testing Methodology
UPS	-	Uninterrupted Power Supply
VAPT	-	Vulnerability Assessment and Penetration Testing
VPN	-	Virtual Private Network
WCAG	-	Web Content Accessibility Guidelines

1. INTRODUCTION

1.1 NABL has taken proactive approach towards accreditation for "Software and IT System Testing". The requirements in this document on specific criteria are based on the International Standard i.e. ISO/IEC 17025: 2017- "General requirements for the competence of testing and calibration laboratories". It specifies requirements for competence and quality that are particular to Software and IT System Testing Laboratories.

This specific criteria document must be used in conjunction with ISO/IEC 17025: 2017. It provides an interpretation of the latter document and describes specific requirements. Further, the laboratory shall follow national, regional, local laws and regulations as applicable.

2. PURPOSE

2.1 Purpose of this document is to specifies the requirement in addition and supplementary to ISO/IEC 17025: 2017 to assess the software and IT System (Software) testing laboratories ensuring quality of Software product/Systems.

3. SCOPE

3.1 This document is applicable for assessing the competence of the laboratory performing the software and IT system testing for test parameters viz. Functionality, Performance/ Efficiency, Usability, Accessibility, Security (Application, Network, VAPT and System), Reliability, Interoperability, Maintainability, Portability, Code review, Conformance (including Unicode) etc.

The software and IT System may include but not limited to the followings:

a) Telecom software/Protocol
b) Embedded systems.
c) Mobile Device and Mobile Applications
d) e-Governance Application and solution Evaluation
e) Gaming Software, Electronic Gaming Machine, Interactive/Internet Gaming products and Systems (i-Game) etc.
f) IOT Block Chain, AI or drone software system/ application
g) Data analytics Software
h) Lottery Software

i) E-Procurement System Software

j) Process and control software

k) Web Application and Website

l) Linguistics Software (if there is linguistic implementation)

m) Sector specific Software & IT system e.g. Defence/ Railways/Banks/ Public sector etc.

n) Software product test & evaluation as per regulatory framework/ guidelines

4. TERMS AND DEFINITIONS

4.1 For the purpose of this document, the definitions and concepts given in ISO/IEC/IEEE 29119-1 shall apply.

 # Note 1: *For the purpose of this document, Software under Testing (SUT), wherever mentioned, shall mean Software and IT System.*

 # Note 2: *The Laboratory/ Institute/ Organization/ Service provider, which possesses the minimum required infrastructure and capability to perform software testing is termed as Software & IT System Testing Laboratory in this document*

5. GENERAL REQUIREMENTS

5.1 Impartiality

a) The laboratory shall clearly define the responsibilities to avoid conflict of interest when the laboratory staff is holding additional responsibilities such as design, development, implementation, operation, maintenance etc. other than testing.

b) When the test scripts and tools are developed as part of the software development process, the laboratory shall have procedures for ensuring its independence and that of its staff from the development process and shall validate its suitability before use to avoid any potential conflict of interest.

5.2 Confidentiality

a) Operational production data containing personally identifiable information or any other confidential information shall be avoided for the purpose of carrying out testing. If personally identifiable information or otherwise confidential information is used as test data, all sensitive details and content are used, it shall be justifiable, masked and protected either by removal or modification.

Refer ISO/IEC 27002: 2003 for guidelines provided under protection of test data (Cl no14.3).

6. STRUCTURAL REQUIREMENTS

a) Laboratory shall comply with the requirements as per ISO/IEC 17025:2017 and relevant NABL policies prevalent at that time.

7. RESOURCE REQUIREMENTS

7.1 General

a) The availability of the resources (personal, environment, facility, Equipment) shall be ensured even while carrying out from or at remote location (other than permanent facility accessing or using Data centre, clouding system and customer environment/ facility).

7.2 Personnel

a) The laboratory shall document the minimum competence requirements for each function such as Test Manager/ Lead and Tester/ Evaluator/ Lead Evaluator etc.

The competency requirements include:

i. Relevant Training, Qualification and Education,
ii. Domain knowledge of the software and IT System being tested,
iii. Knowledge of relevant standard,
iv. Skill of the personal involved in the evaluation/Testing methodology, and
v. Required experience for all the functions.

b) Lab shall identify the appropriate personnel for report, review and authorization to release the test report to the customers.

7.3 Facilities and environmental conditions

a) "Test environment" shall comprise of hardware, reference sample as S/W, H/W standard reference, (e.g. standard finger, standard patterns etc), platforms, middle wares, network, and associated software libraries, drivers etc on which the software being tested is running.

b) Software Testing service may be carried out only in the appropriate test environment that may be created & accessed by following means-

i. **Permanent/ in house testing service:** Test is executed by creating test environment within the laboratory.

ii. **On site Testing:** Test is executed on site location i.e. away from permanent site, by creating test environment accessing IT system infrastructure at customer location or IT infrastructure at Data centres.

iii. **Accessing 'on site testing facility' at permanent laboratory:** Test is executed at permanent laboratory by remotely accessing Test environment that is created either at 'on site customer location' or Data centres or on cloud using IAAS/PAAS services.

In each of the above cases, the laboratory shall maintain and record the configuration of test environment set up throughout the testing process. Measures to control shall be defined and implemented wherever required.

c) In case of In-house testing, where the testing is required to be performed using IT infrastructure or tools or system controlled by the customer/ developer, procedures for the extent of control on these items shall be defined and recorded.

d) Testing shall be performed in a realistic/ similar to production/ target environment relevant to the test parameter and context of use. Deviation, if any, shall be justifiable and the risks due to test environment related specific failures shall be recorded.

e) Testing should be conducted in an environment segregated from both the production and development environment.

f) There should be no other concurrent activities or interference from other activities occurring during testing that may affect or invalidate the results.

g) Where any virtual environment or other special configuration (creating virtual users, setting network bandwidth etc in case of performance/ load testing) is created for simulating real life production conditions, it shall be fully documented in the test records along with a justification as to why it is believed not to affect or invalidate the results.

h) Access control to laboratory areas, server room, Data centre and designated test areas (e.g. Usability Laboratory, Common Criteria laboratory etc) shall be restricted to ensure the integrity of SUTs, test environment and test artefacts.

7.4 Equipment

a) Software Test tools along with its hosting platform and other associated plug-in & add-ons and associated devices/standard required for test are considered as equipment. The laboratory shall have access to equipment and same shall be brought under configuration management.

b) The laboratory shall ensure that current version of test tools and configuration is maintained with regular updation of patches.

c) When the laboratory uses equipment outside its permanent control such as usage of Test tools provided by customer, availing software testing tools on cloud, use of open source tools etc, it shall ensure and maintain records at the time of use but not limited to the followings:

i. Validations of open source tools,
ii. the access control during the test is demonstrable by a document like agreement etc.
iii. The license and version details including patch particulars,
iv. Configuration settings details at the time of use,
v. Repository of automated Test Suite and test data used,
vi. Identity of users and access details,
vii. Type of connectivity Viz. HTTPS, VPN/ IPSec, MPLS/ leased line etc and bandwidth details,
viii. Control of test data (requirement that Software test tools should be reset or logs emptied between tests to ensure that only current test data is recorded)

d) The laboratory shall verify that Software Test tool meets the intended requirements and maintain the records of installation but not limited to the following:

i. Version Number and patch details along with license key details.
ii. Records of verification carried out along with required configuration settings.
iii. Identification of user roles and Access/privilege rights
iv. Configuration details of installation of each instance with unique identification.

e) The laboratory shall maintain records of equipment and shall at least address the following:

i. Identity – each instance of software/hardware.
ii. Supplier/Developer name and version number.
iii. Checks - installation/operational qualifications
iv. Location – target system name or location.
v. Manufacturer's instructions – user manuals.
vi. Validation details.
vii. Up gradation and renewal of license

7.5 Metrological traceability

7.5.1 The test tools including open source tools used by the lab are being validated and the evidences in support of that need to be maintained.

7.6 Externally provided products and services

7.6.1 Externally provided products and services in software testing includes:

a Products:

i. Commercially available software testing tools/ test suites, Configuration Management tools, Test Management Tools, Defect management tools, etc

ii. IT infrastructure such as Servers, Storage devices, Client machines, Network components, etc

iii. System software and Middleware

b Services:

i. Testing tools, IAAS, PAAS services etc on cloud

ii. Internet/leased line connectivity services

iii. Hardware and software/tool maintenance/ up gradation services

iv. Network maintenance services

v. Maintenance of UPS, air conditioners etc.

7.6.2 While availing services such as Cloud services, Internet services, maintenance services, laboratory shall establish requirements in terms of Service level agreement and monitor the performance whether desired level of service is delivered.

8. PROCESS REQUIREMENTS

8.1 Review of requests, tenders and contracts

8.1.1 The procedure for the review of requests, tenders and contracts at least shall address details of Software under Test (SUT): Product Title, Version number, Release details, brief description etc

a) **Test Parameter:** Functional and non-functional testing such as performance/ Security/ usability/ interoperability etc.

b) Test environment and interface requirements including establishing test environment at customer premises, cloud, data centre etc

c) Reporting Methodology.

8.1.2 SRS (Software Requirement Specification), Functional/ Non-functional requirement specification (FRS), Use case document, Business process document, RFP document, Design/ Architecture/interface related documents etc as relevant against which functional/non-functional testing to be performed.

8.1.3 Test methods, Specifications, Standards etc against which test has to be performed viz; CC Criteria Standard, ISO/IEC 15408, GIGW guidelines for Govt web site testing, OWASP for Application Security, etc. Test tool, middleware and Test data requirements.

8.1.4 Retesting/regression testing requirements

8.1.5 Domain/ Technology specific related Training requirements

8.1.6 Acceptance criteria as applicable

8.2 Selection, verification and validation of methods

8.2.1 Software and IT system shall be carried out as per the validated test methodologies/ lab developed methods based upon or drawn from the international/ national/ regional guidelines/ journals/ scientific texts/ publications of relevant reputed technical organizations etc.

8.2.2 Test methodologies/ SOP's shall be documented/ performed/ evaluated so that the expected outcomes and deliverables are achieved as in following examples.

S. No.	Test Process /methodologies	Test Deliverables/ Artifacts	Outcomes
1	Test Planning Process	Test Plan	- scope of testing - Risk that can be treated by testing are identified, analysed and classified - Test strategy, test environment, test tool and test data needs are identified; - Resource, training and staffing needs - Analysis, design, implementation, execution and reporting schedule - Exit criteria
2	Test Design and Implementation	- Test Design Specification - Test case design - Test Procedure Specification	- The test basis for each test item is analysed; - The features to be tested are combined into Feature Sets - The Test Conditions are derived - The Test Coverage Items are derived; - Test Cases are derived; - Test Sets are assembled; - Test Procedures are derived

3	Test Execution Process	- Test Execution log - Test Results	- Execute Test Procedure(s) - Compare Test Results - Record Test Execution
4	Test Incident Reporting Process	Test Incident reporting	- Test results are analysed - Incidents are confirmed - Incident report created/updated - The status and details of previously-raised incidents are determined;

8.2.3 The selection and combination of Test Design techniques/ Test methods shall ensure that:

a) Test case results are not ambiguous and have single thread of execution with objective results relating to expected outcomes.

b) The traceability between the test basis, feature sets, test conditions, test coverage items, test cases, test sets and test procedures (and/or automated test scripts) exists and is recorded.

c) The laboratory shall periodically review and approve the test artefacts such as Test plan, Test design specification, Test cases, Test procedures (and/or automated test scripts), Test logs and test incident report before execution or release.

d) All test artefacts shall be brought under configuration management.

8.3 Sampling

8.3.1 The sampling is not for selection of product for testing. The sampling in IT activities shall be done to optimize the Test activities.

8.3.2 Test strategy/ approach shall determine the extent of sampling in terms of test analysis and activities to be performed based on the context and risk of testing. The laboratory shall establish and confirm the extent of sampling by creating the test artefacts as relevant but not limited to the following:

a) Test Plan specifying the risk, strategy/ approach of testing, test techniques to be used, exit criteria, etc.

b) Test design specification specifying either the features/functions/transaction/quality attribute or structural element to be tested and their corresponding test conditions.

c) Test case specification specifying selection and prioritization of test cases, etc

d) Extent and Selection of regression tests to rerun;

e) Selection of source code to review based on risk.

8.4 Handling of test items

a) SUT shall be clearly identified with its version number along with the release note of SUT as applicable from the customer.

b) Any subsequent testing after defects are fixed shall be carried out only after SUT is submitted with clear identification of different version.

c) In case of installation problems such as compatibility with middleware, libraries, etc and/or integration with other systems, system software etc, the laboratory shall record the same and customer shall be accordingly intimated for further instructions before proceeding.

d) Maintain & record the configuration management with appropriate metadata to ensure it is unique. Test base documents pertaining to SUT such as SRS, FRS, use case document, RFP, design/ architecture/ interface documents etc shall also be brought under configuration management.

e) The laboratory shall ensure integrity of the SUT and shall establish method to verify throughout the test life cycle. It shall be protected from unauthorized/ unintended modification or changes during normal installation process, integration with other systems/tools, testing process, etc.

f) In case an unintended modification occurs in the test item software or gets corrupted, the software shall be re-installed to its initial state before resuming the test.

g) Access to the Test environment and SUT shall be controlled.

h) Laboratory shall ensure that the integrity of SUT and test environment is maintained throughout test life cycle when installed outside laboratory's control such as in Data centre, cloud, customer premise etc.

8.5 Technical records

a) Technical records include all test deliverables/ artefacts as listed at 8.2.1 which are produced during testing besides Test environment set up details, equipment/ tools details, SUT and its allied documents, contract review records, etc.

b) All technical records shall be brought under configuration management. Access to technical records shall be controlled and privileged rights shall be defined.

8.6 Ensuring the validity of results

a) The procedure for monitoring the validity of results shall address the following and records shall be maintained as practicable:

i. Periodic review of Test plan covering Test strategy, Risk, scope, schedule and resources.

ii. Periodic review of Test design specification and Test case design records verifying for appropriateness of Test condition/scenario selection, Test method selection, test coverage with back and forth traceability, Test environment set up, Test tool selection, granularity of testing etc.

iii. Review of Test execution logs and incident reporting.

iv. Review of false positives in the report generated by automated tools.

v. Functional check(s) and intermediate checks of Test tools.

vi. Review of regression Test suites.

8.7 Reporting of results

In addition to the requirement of Clause 7.8 of ISO/IEC 17025: 2017 following may be included wherever applicable:

i. In case of multiple reports issued for same SUT such as separate report for functionality, security, performance, Usability, interoperability, etc, the laboratory shall ensure linkage between the reports confirming the test requirements as per the contract review.

ii. Description of open defects in an unambiguous way

iii. Traceability of test results with requirements and/or specifications

iv. Information on specific test conditions and simulation criteria

v. Deployment (In-house, cloud, data centre etc) and configuration details of test environmental set up including mode of access.

vi. Reference to Test methods including any deviations or exclusions

vii. Details of Test tools along with version and patch details and any configuration settings if any

viii. Methodology used for Severity Classification for Software anomalies such as IEEE 1044, user requirement, etc

ix. Methodology used for Regression testing.

9. ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES

a) Depending upon the context, constraints and type of testing, the laboratory shall adopt appropriate risk-based approach to testing. Risk identification and analysis methodology as relevant may be adopted so that the perceived risks in the developed/delivered system are identified, scored, prioritized and subsequently mitigated.

b) The laboratory shall identify and address risk in test plan by specifying appropriate risk mitigation strategy and approach to testing.

c) The laboratory shall evaluate the effectiveness of risk implementation by implementing actions such as review of test plan, review of test coverage, evaluation of test exit criteria, etc.

Note : *In context of software testing, the risks may exist/ arise at any stage/ action e.g. risks of not satisfying regulatory and/or legal requirements, failing to meet contractual obligations, criticality of the product, non-availability/ scarcity of required infrastructure, lacking simulation of real testing environment, delivery schedule, emergency or random work load leading to unsatisfactory progress of activity/project (project risks) and risks due to system upgrade, use of new/ migrated technologies and work product not achieving its expected behavior (product risks).*

9. SAMPLE SCOPE (EXAMPLE)

S. No.	Materials or Products tested	Component, parameter or characteristic tested/ Specific Test Performed/ Tests or type of tests performed	Test Method Specification against which tests are performed and/or the techniques/ equipment used	Range of Testing/ Limits of detection	Uncertainty of Measurement (±) at Value
1	*Software System and Application (e-governance, Telecom Software etc.)	Functional Testing	ISO/IEC/IEEE 29119-4.	Qualitative	NA
		Application Security Testing	OWASP: 2017 CWE-25	Qualitative	NA
		E Governance Website testing	GIGW Guidelines	Qualitative	NA
		Usability Testing & Heuristic Evaluation (Human – System Interaction Analysis)	ISO/IEC 9241, ISO IEC 9126-2	(Qualitative	NA
		Static Code Review, Inspection & Maintainability Analysis	IEEE 1028, IEEE 1044; MISRA Guidelines	Qualitative	NA
		Performance testing	TM/abc/xyz	Qualitative	NA
		Accessibility Testing	WCAG 2.0 Guidelines	Qualitative	NA
2	Computer Networks	Vulnerability Assessment, Non-Destructive Penetration Testing	CIS; NIST SP 800-115; TM/abc/xyz	Qualitative	NA
3	Boundary Protection Devices, Access Control Devices etc	Class: ASE – Security Target Evaluation ADV – Development AGD – Guidance Documents ALC – Life-cycle support ATE – Tests AVA – Vulnerability Assessment Class: APE – Protection Profile Evaluation Functional Testing; Independent Verification and Validation; Security Assurance Evaluation (EAL 1 & 2)	ISO/IEC 15408: Evaluation Criteria for IT Security Part 1: Introduction and General Model; Part 2: Security Functional Requirements; Part 3: Security Assurance Requirements	Qualitative	NA

Note: NABL 130 shall be referred while recommending the scope for site.

*Or any other application Software, for which laboratory is seeking accreditation, is to be categorically specified.

10. REFERENCES

I. ISO/IEC/IEEE 29119: Software and systems engineering — Software testing:
Part 1: Concepts and definitions
Part 2: Test processes
Part 3: Test documentation
Part 4: Test techniques

II. ISO/IEC 25010: Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models

III. ISO/IEC 25051: Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) —Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing.

IV. Refer ISO/IEC 27002: for guidelines provided under protection of test data (Cl no14.3).

V. ISO/IEC 16085: Systems and software engineering — Life cycle processes — Risk management

VI. IEEE 1044-2009 - IEEE Standard Classification for Software.

National Accreditation Board for Testing and Calibration Laboratories (NABL)
NABL House
Plot No. 45, Sector 44,
Gurgaon - 122003, Haryana
Tel. no.: 91-124-4679700 (30 lines)
Fax: 91-124-4679799
Website: www.nabl-india.org