Procedure for Assessment of System and Software

May, 2014

STQC - IT Services

STQC Directorate, Department of Electronics and Information Technology,

Ministry of Communications & Information Technology,

Electronics Niketan, 6 CGO Complex, Lodi Road,

New Delhi – 110003.

1.0 Introduction & Overview:

1.1 Background:

STQC is involved in a large number of IT projects of various sizes & scales as independent third party Conformity Assessment Agency. The conformity assessment is primarily carried out using Review, Testing & Audit techniques.

The conformity assessment by STQC mainly involves Conformity Assessment & Quality Evaluation of IT projects which primarily comprises of reviews, testing & audit of various key project components covering Website/ Portal, Software Application, Project Documentation, Project Processes, IT Infrastructure (including Hardware, Software and Network deployed at Data Center, Disaster Recovery, Front/ Back offices), Data Quality. The conformity assessment is carried out to evaluate the key quality attributes like Functionality, Performance, Security, Usability, Maintainability, Service Quality etc.

The conformity assessment services offered by STQC are:

- Architecture Review & Audit
- Software Application Testing
  - Functional
  - Non-functional (performance, Security, Usability, etc.)
- Information Security Audit & Testing
  - Application Security;
  - Vulnerability Assessment;
  - Penetration Testing
- Documentation Review (Processes & Products)
  - Policies & Procedures and Software Documentation
- Process Audit
  - Design, Development, Operation & Maintenance Life cycle Processes;
  - Information Security Management Processes;
  - IT Service Management Processes
- IT & Non IT Infrastructure Audit
  - DC, DR, GW, NW, HW + Facilities (FO & BO)
- Service Quality (SLA Compliance)
  - SLA Measurements
  - SLA Measurement System Audit

The conformity assessment activities (i.e., Review/ Testing/ Audit) are carried out by STQC at different phases/ stages of the IT projects such as pilot, pre-Go-live and post Go-live phases/ stages in the staging or production environment.

1.2 Basic Principles:

The conformity assessment is based on following principles:

- Independent third party (Objectivity) assessment
- Use of International Standards & best practices
- Use validated assessment methodologies & techniques
- Ensure that assessment result are reliable, repeatable & reproducible

1.3 Issues:

The present approach of conformity assessment is very elaborate way of evaluating the key components of the IT projects. However, there are certain constraints and limitations listed below:

Constraints & Limitations:

- The complete & correct information about the system and software required by STQC is not provided in time by the Implementation Agency (IA).
- The system and software is not thoroughly verified by client &/or developer for readiness before offering it to STQC.
- Project in general is already behind the schedule, at the time when STQC gets involved.
- Limited exposure of business domain & technologies used to STQC team.

In order to resolve these issues an alternate approach is being suggested here so that STQC activities can be taken up on fast track mode without compromising the overall quality of work. The assessment take up by STQC using this approach will be based on combination of:

a) Verification of testing process and procedures (including test planning, test case designing, test execution and test reports) of IA for compliance with testing standards.
b) Demonstration of testing carried out by IA for compliance (coverage and depth of testing) with project requirements.
c) Sample testing by STQC assessment team.

It will provide the same level of confidence as give by independent third party testing.

1.4 Basis of Approach Suggested:

The approach proposed will help reducing the time taken by STQC in familiarization and understanding the IT system and software. The primary assessment technique suggested is system and software audit (ISO/ IEC 12207-2008, clause 7.2.7.3.2 Software Audit) although it will be combined with limited review (IEEE Std 1028-1997, IEEE Standard for Software Reviews) and testing (ISO/IEC 25051 (new) Software Engineering: Software Product Quality Requirements and Evaluation (SQuaRE) - Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing) techniques as well.

The basis for adopting the approach is based on the Software Audit Process defined in the International standard ISO/IEC 12207 (IEEE Std 12207-2008) - Systems and software engineering - Software life cycle processes.
The purpose of the Software Audit Process is to ***independently determine compliance of selected products and processes with the requirements, plans and agreement, as appropriate***.

As a result of successful implementation of the Software Audit Process:
a) An audit strategy is developed and implemented;
b) ***Compliance of selected software work products and/or services or processes with requirements, plans and agreement*** is determined according to the audit strategy;
c) Audits are conducted by an appropriate independent party; and
d) Problems detected during an audit are identified and communicated to those responsible for corrective action, and resolution.

Software audit is conducted to ensure that:
a) As coded, software products (such as a software item) reflect the design documentation.
b) The ***acceptance review and testing requirements prescribed by the documentation are adequate for the acceptance of the software products***.
c) Test data comply with the specification.
d) ***Software products were successfully tested and meet their specifications***.
e) ***Test reports are correct and discrepancies between actual and expected results have been resolved***.
f) ***User documentation complies with standards as specified***.
g) Activities have been conducted according to applicable requirements, plans, and contract.

In addition it is recommended that User Acceptance Testing (UAT) of the system/ software is also carried out by the end-users.

2.0 Purpose & Objectives:

The primary purpose of carrying out Assessment & Evaluation (mainly through audit technique) of the system and software is to assure quality from user's viewpoint and provide confidence to users.

The key objectives of the assessment by STQC are to verify:

- Compliance to Project Objectives & RFP/ Contract Requirements
- Fulfillment of quality characteristics
- Adherence to applicable regulations, standards and specifications set out in the RFP
- Timely identification & fixing of anomalies (defects/ nonconformities/ issues) in the system and software

3.0 Scope:

The assessment will primarily cover system & software of the IT project. However, same approach may be used for assessment of other project components such as project documentation, processes, Software, Hardware, Network, SLAs, etc.

4.0 Responsibilities:

The assessment team will be comprised of following members from STQC:

Lead Assessor:

- Overall management the team
- Assist in team selection
- Preparation of audit programme/ checklist
- Control over the team's work
- Interfacing with the auditee management
- Preparation/ submission of audit report
- Audit conduction

Assessor:

- Communicate audit requirements
- Be effective & efficient
- Document observations
- Report Results
- Verify corrective action effectiveness
- Remain within scope
- Support other team members

Implementation Agency (IA):

IA provides development, operation and maintenance services to project and will be responsible for followings:

- Making the required inputs available to STQC
- Ensure readiness of the system to be verified and timely provide the documentation and the required information to STQC.
- Provide access of the system to STQC
- Initiate timely action to fix the anomaly (defects/ nonconformities) reported
- Demonstrate the satisfactory closures of the reported anomaly (defects/ nonconformities)

IA may himself be a client in some cases.

Auditee (Client):

The client of the system will support the STQC team in the following activities:

- Initiates the assessment process through a request.
- Act as interface between STQC & IA
- Provide domain expertise
- Provide support & assistance during assessment

5.0 Assessment Approach:

The approach to be followed for assessment is essentially based on combination of review, testing & audit techniques, though primary focus on audit methodology. Assessment will

Assessment will be performed to:

- Verify the documentation for adequacy of description & details as per RFP/ Compliance Criteria
- Verify Completeness, Correctness, Clarity & Consistency of system and software documents such as requirements and user documentation.
- Verify Traceability of documents to previous and later phases of the project.
- Check that the system/ software are in the state of readiness for the assessment by STQC (i.e., the system/ software is fully developed, internally verified and deployed). Also check that the system/ software is deployed on the required platform (hardware and software configurations).
- Verify that all the requirements are implemented as per specified requirements in the RFP/ Compliance Criteria
- Verify the internal QA activities of IA (various review/ test/ audit records of IA)
- Demonstration of execution of test cases by IA.
- Independent testing by STQC on business critical functions on sample basis.
- Verify Compliance with applicable Standards & Regulations
- Identify anomalies & ensure that they are addressed before system and software is deployed.
- Verify adequacy, implementation and effectiveness of defined practices/ processes as per applicable requirements & standards

The assessment approach is described in detail below:

Assessment - Steps:

Assessment cycle will consist of following steps:

A. Study & Preparation
B. Planning
C. Execution
D. Reporting
   Corrective action will be taken by IA on the reported defects/ nonconformities
E. Verification & closure of reported anomalies (defects/ Non-conformities)
F. Final Report

Inputs Required for Assessment:

Assessment will required following minimum inputs:

- RFP/ Compliance Criteria Documents
- Requirements Document
- Traceability between RFP & Requirements Document
- Test Documentation including Test Plan, Test Cases and Test Reports

Assessment - Activities & Tasks:

Assessment consisting of following activities and tasks will be undertaken:

A) Study & Preparation:

- Study & understand the project requirements from RFP
- Study requirements document & understand the system & software requirements.
- Study & understand system and software documentation (UM and related information), documentation structure and relationships.

B) Planning:

- Work out & finalize assessment methodology.
- Decide about assessment locations & environment in consultation with client/ IA.
- Appoint assessment team members
- Prepare assessment checklist & criteria/ audit objectives
- Prepare & communicate the assessment schedule

C) Execution:

- Review the system and software documentation.
- Carryout traceability check (mapping) between requirements as given in the RFP and system and software document.
- Verify correctness, completeness, clarity, consistency, traceability & Document control of document.
- Record document review observations/ logs.
- Get the demonstration of the system and software from IA.
- Walk through and check whether the system and software is fully functional and is in state of readiness.
- Identify the critical business areas/ functions (high risk) in consultation with users and carryout detailed verification (through test cases of STQC). Generally these critical business functions should not be more that 15% of the overall software functionalities.
- Verify that system and software functions are in compliance with the specified functional requirements and identify defects/ issues (if any).
- Verify system and software documents, logs, reports & records
- Also verify compliance to applicable regulations, standards and specifications set out in the RFP.
- Collect information and analyze
- Record the assessment observations/ logs.

D) Reporting:

- Analyze the assessment observations/ logs.
- Identify anomalies/ issues & assign severity/ risk.
- Prepare Anomaly (defect/ non-conformance) Report & submit to client/ IA.
- IA to initiate corrective action on the reported anomaly and submit Corrective Action Report to STQC.

E) Verification & Closure:

- Verify corrective action (Resolution/ fixing) of the reported anomaly for closure from the Corrective Action Report.
- Carryout re-assessment of the system and software.
- Record the assessment observations/ logs.
- Prepare Final Report.

Anomalies identified will be classified in terms of severity as follows:

Anomaly Severity	Description
Urgent	• The failure causes a system crash or unrecoverable data loss or jeopardizes personnel. • Absence of the document, i.e., document not available (missing). • Absence or total breakdown of process requirement.
High	• The failure causes impairment of critical system functions and no workaround solution exists. • Critical information/ contents of the document completely or partially missing/ wrong/ misleading. The defect/ deviation is given high attention to resolve on priority. • Critical requirement is completely or partially missing/ wrong/ misleading. The defect/ deviation is given high attention to resolve on priority
Medium	• The failure causes impairment of critical system functions, though a workaround solution does exist.

	• Significant defect/ deviation to comply with documentation requirement. • Significant failure to comply with specified process requirement.
Low	• The failure causes inconvenience or annoyance. • Single observed isolated lapse in the document. A minor problem having negligible effect on document quality & warranting attention. • Single observed isolated lapse of a process requirement. A minor problem having negligible effect on quality & warranting attention
None	• None of the above, or the anomaly concerns an enhancement rather than a failure & anomaly.

Usage of Tools:

STQC may use various automated tools for carrying out assessment activities as follows:

a) Static analyzer tools (Logiscope, MS fxcop, etc.) for code analysis.
b) Performance test tool (HP Load Runner, Slik Performer, etc.)
c) Application security test tools (IBM Appscan, Paros, etc.)
d) Web site test tools (IBM Rational Policy Tester)
e) Vulnerability Assessment and Network audit tools (Nessus, nmap, Saint)
f) Measurement of technology related SLAs (HP Load Runner, Slik Performer, etc.)

To undertake assessment activities & tasks, STQC team will be provided with access to system, various documents and associated information. STQC team will also be allowed access to hardware, software, Network & IT infrastructure and processes of the system and also to connect test/ audit tools on to the system, wherever required.

Output Produced by Assessment:

- Anomaly Report (Defect/ Nonconformity)
- Closure Report (by IA)
- Final Report

Annexure I

Definitions and Explanations

Software Audit: is software review in which one or more auditors who are not the members of the software development organization conduct "An independent examination of software product, software process(s), or a combination of these to assess compliance with specifications, standards, contractual agreement or other criteria."

Software Product: include technical document (IEEE std 1028 refers a list of 32 examples of software product subject to audit) like plans, contracts, specifications, designs, procedures, standards and reports, but also non-documentary products such as data, test data, deliverable media etc.

Establish: Mean to "define, document, and implement".

Requirements and Specifications:
Requirements: Generally Quality System states that design input requirements must be documented, and that specified requirements must be verified. The distinction between the terms "requirement" and "specification" is not further clarified.
Specification: A specification is defined as "a document that states requirements". It may refer to or include drawings, patterns, or other relevant documents and usually indicates the means and the criteria whereby conformity with the requirement can be checked. There are many different kinds of written specification, e.g. system requirements specification, software requirement specification, software design specification, software test specification, software integration specification etc. All of these documents establish "Specified requirements" and are design outputs for which various forms of verification are necessary.

Verification and Validation:
Verification: provides objective evidence that the design outputs of a particular phase of the software development life cycle meet all of the specified requirements for that phase. It looks for consistency, completeness and correctness of the software and supporting documentation, as it is being developed and provides support for a subsequent conclusion that software is validated.
Validation: it is a part of the design validation for a finished device "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled. In practice software validation activities may occur both during as well as the end of the software development life cycle to ensure that all requirements have been fulfilled.

Annexure II

Overview of ISO/IEC 25051

- ISO/IEC25051: Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing.
- Scope(who can use this standard):
  - Certification bodies that may wish to establish a third-party certification scheme (international, regional or national) (ISO/IEC Guide 28);
  - Requirements for conformity assessment are:
    - Clause 5.1 Product Description
    - Clause 5.2 Requirements for user documentation
    - Clause 5.3 Quality requirements for software
    - Clause 6.0 Requirements for test documentation
- Clause 6. Requirements for test documentation:
  The test documentation shall contain:
  a) The test plan;
  b) The test description;
  c) Test procedures
  d) The tests results
  e) Anomaly Report
- Clause 7.3.3 Software conformity evaluation:
  Conformity evaluation:
  7.3.1 Product description conformity evaluation
  7.3.2 User documentation conformity evaluation
  - For 7.3.1 and 7.3.2 no specific techniques or tools are recommended.
  - The Standard suggests review of the test documentation including the descriptive part for the anomalies found
- Clause 7.5 Conformity evaluation report
  - The COTS software product identification;
  - The date of evaluation completion and, if any, testing completion;
  - The computer systems used for testing (hardware, software, and their configuration
  - The documents used, with their identification;
  - The summary of conformity evaluation activities and, if any, testing activities;
  - The summary of conformity evaluation results and, if any, testing results;
  - The detailed results of conformity evaluation and, if any, testing;
  - The list of non-conformities to requirements if any.
- Clause 7 Software conformity evaluation:
  Clause 7.0 discusses the conformity assessment processes and gives two alternatives:
  1. If the supplier provides only the COTS software product, without the test documentation, the third-party shall:
     a. Carry out a conformity evaluation of the product description, the user documentation, and the software according to subclause 7.3;
     b. Record the results in a conformity evaluation report, according to subclause 7.5.
  2. If the supplier provides the COTS software product and the test documentation, the third-party shall:
     a. Carry out a conformity evaluation of the product description and the user documentation according to subclauses 7.3.1 and 7.3.2;
     b. Carry out a conformity evaluation to determine the conformity of the test documentation to the requirements in Clause 6;
     c. Record the results in a conformity evaluation report, according to subclause 7.5.

Annexure III

Template for Test Cases/ Scenarios and Test Log

Software Nomenclature:
(Name, Version)

Test Scenario & Test Cases:

Test Scenarios:

Test Scenario1: <Test Scenario Name>

Test Scenario Description:

Pre-conditions:

Sr. No.	Test Step	Test Step Description	Expected Output	Actual Output	Result
1.					
2.					
--					

Note: The test data for test steps of the test scenarios should be prepared in the following table.

Comments:

Test Cases & Test Data:

Test Step:

Sr. No.	Test Data (Valid/ Invalid)	Test data						Expected Output	Actual Output	Result
		Field 1	Field 2	-	-	Field n	Action			
1.										
2.										
--										

Comments:

Note:

- Prepare the test scenario (as per table 3.1 above) describing the test steps for the test scenario using specified workflows, navigations & other relevant information for the software.
- For the test steps, wherever required, define the test cases along with test data (as per table 3.2 above) using the specified business logic/ rules, validation rules & other relevant information for the software.
- For test execution, start with test steps given in the test scenario, and use test cases with appropriate test data from the corresponding to the test case table.
- Test results as observed for each of the test step as well as test cases should be recorded the "Actual Output" field of the tables 3.1 & 3.2.
- In case of defect, the details of observations with complete details (to allow traceability & repeatability) should be recorded in the "Actual Output" field in the tables. Also screen shot may be captured and stored.
- The "Actual Output" should be recorded with adequate details so as to help to create test observations.
- From the test observations, defects/ problems/ issues should be identified and recorded in the test log below.

Test Log

Software Nomenclature:
(Name, Version)

Test Observations:

Software Module:
Tested By & Date:

Sr. No.	Function/ Parameter	Document Reference (SRS/UM)	Test Observations	Defect/ Problem/ Issue
1.				
2.				
--				

Note: Where required screen shot of the defect may be attached to support the test observations.

Comments:

Annexure IV

Anomaly Report Template

Software Nomenclature:
(Name, Version)

. Test Results:

Anomaly Summary:

Sr. No.	Defect Severity	Software Module - Number of Defects						Total Defects
1.	Urgent							
2.	High							
3.	Medium							
4.	Low							
5.	None							
Total Defects								

Defect Severity:

Defect Severity	Description
Urgent	The failure causes a system crash or unrecoverable data loss or jeopardizes personnel.
High	The failure causes impairment of critical system functions and no workaround solution exists.
Medium	The failure causes impairment of critical system functions, though a workaround solution does exist.
Low	The failure causes inconvenience or annoyance.
None	None of the above or the anomaly concerns an enhancement rather than a failure.

Anomaly Details:

Software Module:
Tested By & Date:

Sr. No.	Function/ Parameter	Document Reference (SRS/UM)	Defect Description	Defect Severity
1.				
2.				
--				

Note: Where required screen shot of the defect should be attached.
Comments:

Annexure V

Test Report Template

Software Nomenclature:
(Name, Version)

. Test Results:

Test Results - Functional Testing:

Functional Test Observations:

Software Module:
Tested By & Date:

Sr. No.	Function/ Parameter	Document Reference (SRS/UM)	Specified Requirement & Conditions	Observation	Result
1.					
2.					
--					

Comments:

Defect Summary:

Sr. No.	Defect Severity	Software Module - Number of Defects						Total Defects
1.	Urgent							
2.	High							
3.	Medium							
4.	Low							
5.	None							
Total Defects								

Defect Severity:

Defect Severity	Description
Urgent	The failure causes a system crash or unrecoverable data loss or jeopardizes personnel.
High	The failure causes impairment of critical system functions and no workaround solution exists.
Medium	The failure causes impairment of critical system functions, though a workaround solution does exist.
Low	The failure causes inconvenience or annoyance.
None	None of the above or the anomaly concerns an enhancement rather than a failure.

Defect Details:
Software Module:
Tested By & Date:

Sr. No.	Defect Description	Defect Severity
1.		
2.		