Procedural Guidelines for Certification including Maintenance of Certification

Of STQC Certified e-Procurement System

Document Version : 1.0 dated 02nd February 2018

The comprehensive scheme for software and System certification by Standardization Testing & Quality Certification Directorate (STQC) 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.

E-Procurement Systems certification activities are undertaken by various STQC IT Centres as per the guideline document issued by Ministry of Electronics & IT.

The EPS testing & evaluation activities, being comprehensive, generally take 2-3 months time. Based on the experience gained since the launch of the scheme and feedback from certified organisations and other stakeholders, the procedure and process of certification activities have been amended.

The key aspects of amended procedural guidelines are :

1. **Statement of Conformity Certification validity : 3 years**
2. **Surveillance audit : at the end of 1st and 2nd year.**
3. **In surveillance following activities need to be audited:**

a. **EPS and related documentation** is NOT changed
   - declaration by certified client organization is must

b. **Application Security and Network Security Assessment** :
   (i) Application security report- by STQC or CERT-IN empanelled agency
   (ii) Hardening of servers & network devices Report – STQC or CERT-IN empanelled Agency
   iii) Vulnerability Assessment of servers and network devices if only 'hardening of servers and network devices report' is consulted /reviewed (without Security Vulnerability scanning) then we must look into the logs of patching the servers, However, full VA is preferable]
   iv) Penetration Testing

c. **List of client** (If, there are multiple clients) –to be submitted by certified Organisation

d. **Details of feedback or complaint** received

e. Review of the **state of continuation of ISO 27001 certificate** for system (if used during initial certification)- not applicable when scope is limited to e procurement application*)*

Operational Mechanism for Surveillance/Re-certification:

1) The certified organisation shall contact STQC Certification body/laboratory within 12 months of initial certification (preferably one month in advance) with necessary inputs, as given above, for surveillance.

2) Upon satisfactory report from STQC testing laboratory, a statement of **"Continuity of Certificate"** shall be issued by certification body.

3) Certified client shall ensure timely completion of Surveillance audits. Non-compliance to surveillance time schedule may lead to suspension/withdrawal of certification.

4) For Re-certification, the certified clients need to apply for certification at least 3-4 months before the expiry date of initial certification to STQC testing lab/Certification body.

****