Procedural Guidelines for Surveillance Audit of STQC Certified e-Procurement Systems

Document Version: 2.0 **dated** May 2024

The comprehensive scheme for eProcurement System (EPS) certification by Standardization Testing & Quality Certification Directorate (STQC) involves Conformity Assessment & Quality Evaluation of EPS products 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.

E-Procurement Systems testing activities are undertaken by various STQC IT Centres as per the guideline document issued by Ministry of Electronics & IT. eProcurement System Certificate is issued for a duration of three years with the condition of completion of the surveillance audit at the end of 1st and 2nd year. Surveillance audit shall be conducted by an STQC auditor nominated by the Certification Body (CB). Surveillance audit date will be communicated to the EPS customer 2-3 months in advance. Surveillance audit shall be conducted in physical mode (Not Online). Customer must ensure that they are ready with the required test artefacts before the surveillance audit dates.

In case of any changes in the certified eProcurement system, it is mandatory for the customer to list all the changes along with their impact on Functionality, Security, CVC/IT Act, Infrastructure and Performance in the impact assessment form (Annexure I). If there are no changes in the application, then customer need to give a declaration regarding no change in the eProcurement System.

Impact assessment form will be reviewed by the CB nominated auditor and the auditor shall verify the correctness of the changes and their impacts on Functionality, Security, CVC/IT Act, Infrastructure and Performance. If any deviations are found by the auditor which necessitates recertification of the eProcurement system, the auditor shall mention the same in their report submitted to the CB. Only major changes which affect core functionality, security or infrastructure of the eProcurement system, will lead to recertification. Decision for recertification will be taken by CB after considering STQC nominated auditor's report. Apart from recommendation for recertification, if any other deviation is observed by the auditor, the customer shall be given a period of three months to rectify the deviations. If the customer is not able to rectify the deviations within three months of the audit, the certificate shall be withdrawn.

Guidelines for the Customer: The customer shall ensure that they are ready with the test artefacts before the audit date. List of test artefacts which should be kept ready are as follows:

1. Application Security Test Report- by STQC Lab or SETL (STQC Empaneled Test Laboratory) (Not older than six months on the day of Surveillance Audit).
2. Vulnerability Assessment of servers and network devices by STQC or SETL (Not older than six months on the day of Surveillance Audit).
3. Impact Analysis Form (Annexure I)/No Change Declaration
4. List of clients (If, there are multiple clients) –to be submitted by the customer.
5. Details of feedback or complaint received.
6. Review of the state of continuation of ISO 27001 certificate for system (if used during initial certification)

Guidelines for the Auditor: The auditor shall conduct physical audit (1 day) and conduct the audit as per the surveillance audit checklist (Annexure II). Auditor shall submit their report to CB. The main aim of the audit is to verify if the customer has the latest application security test report, vulnerability test report, and to verify if the change management/release management process is in place. One man day audit charges shall be levied for the audit. (Note: These are only audit charges and do not include charges for Application Security testing & Vulnerability Assessment). The proposal for the audit shall be shared by the STQC nominated auditor's lab and the payment shall be collected by the corresponding lab.

Validity of the certificate and the surveillance audit timelines

1. Statement of Conformity Certification validity : 3 years
2. Surveillance audit : at the end of 1st and 2nd year.

Annexure I

Format for Impact Analysis for Changes in e-Procurement Application/ e-Procurement System

Client name:
Certificate No:
Surveillance 1/Surveillance 2:

S.no.	Details of change (module/Infrastructure etc)	Reason of Change	Details of Change in Functionality	Impact on overall functionality (No impact (NI)/ No significant impact (NSI)/ significant impact (SI))					Remarks
				Functionality	Security	CVC/ IT	Infrastructure	performance	

Certificate regarding Changes (by applicant/client):

It is certified that the impact of changes on Security/ Functionality/ Infrastructure/ Performance / CVC IT requirements have been evaluated with respect to initial certification and:

1) *There are no significant changes in application/system
2) *There are significant changes in application/system functionality/Security/Infrastructure/ CVC IT with respect to the initial system tested and certified.

(* strike off which is not applicable)

Signature of Authorized Signatory (Applicant)
Name:
Designation:
Date: Place:

Note: Please attach all background papers for justification

Valid Recommendations of the STQC Nominated Auditor:

(The Auditor should verify impact analysis done by the client and clearly indicate their agreement / disagreement with it in their recommendation below.)

_____
_____

Signatures
Name:
Designation:
Date: Place:

Annexure II

Surveillance Audit Checklist

Sr. No.	Surveillance Audit Requirement	Compliance Status	Remarks/Observations
1.	Is Filled and Signed Impact Analysis submitted by the client? (No change declaration in case of no changes in eProcurement System)		
2.	Is Impact Analysis reviewed by the Auditor? If yes, please provide comments/observations.		
3.	Is impact of changes mentioned in the Impact Analysis Form reviewed by the Auditor? Please provide remarks/observations.		
4.	Application security report available? (Not older than six months). Please Mention report issued date.		
5.	Any open issue in application security report?		
6.	Vulnerability Assessment report available? (Not older than six months) Please Mention report issued date.		
7.	Any open issue in Vulnerability Assessment report?		
8.	Verify if the organization has implemented change management policy?		
9.	If yes at above, is the list of changes mentioned in Impact Analysis identifiable through change management process?		
10.	Is there any change in application version due to changes? If yes, is it a major change or a minor change?		
11.	Is classification of change available (Major/Minor)?		
12.	Are details of Configuration Item captured in change management?		
13.	Verify if backup policy is in place and if it is strictly being followed? (Verify Backup Logs)		
14.	Verify if patch management policy is available and verify if latest updates and patches are applied to all the servers and network components?		
15.	Any negative feedback or complaint received by the customer? If yes, did customer take any action on the feedback/complaint? Please provide details		
16.	Verify if DC & DR ISMS certificates are still valid		