Digital Platform Conformity Assessment

Version 1.0

9th September, 2020

STQC Directorate,
Ministry of Electronics & Information Technology,
Electronics Niketan, 6 CGO Complex, Lodi Road,
New Delhi – 110003.

Digital Platform Conformity Assessment

Table of Contents

1.0 Introduction:

1.1 Background:

Digital India programme is a flagship programme of Government of India with a vision to transform India into digitally empowered society and knowledge economy. The Digital India programme weaves together various government schemes, many of which cut across all the Central Ministry/ Departments. The programme is to be implemented by the entire government both Central, State/UT and coordinated by Ministry of Electronics and Information Technology (MeitY)

The vision of Digital India programme is to transform India into a digitally empowered society and knowledge economy:

- Digital Infrastructure as a Core Utility to Every Citizen
- Governance & Services on Demand
- Digital Empowerment of Citizens

The Digital India vision aims to "Make all Government Services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency and reliability of such services at affordable costs to realize the basic needs of the common man".

To realize this vision, MeitY enable and facilitate rapid introduction of Digital India in the country, with focus on service delivery. As per the implementation strategy, an identified line Ministry/ Department would define the service and service levels of their respective Projects and develop detailed guidelines for achieving the same.

1.2 Objectives:

Digital India is to provide the thrust to the nine pillars of growth areas, namely Broadband Highways, Universal Access to Mobile Connectivity, Public Internet Access Programme, Digital India: Reforming Government through Technology, e-Kranti - Electronic Delivery of Services, Information for All, Electronics Manufacturing, IT for Jobs and Early Harvest Programmes. Each of these areas is a complex programme in itself and cuts across multiple Ministries and Departments.

It has targeted certain high volume services delivered, and undertake backend computerization to e enable the delivery of these services through Common Service Centres in a sustainable manner, within a specific time frame.

The Digital India has been formulated that:

- Quality and content of Government Service Delivery can significantly improve with an integrated approach to service delivery.
- Capacity building of the administrative functions and processes will enhance efficiency and accountability in service delivery.
- The services which would be delivered would have automated work flow and would perforce involve significant process redesign.
- A Central data repository would be created, wherein data and information would be collected, stored, retrieved, used and exchanged in an efficient manner at all levels.
- Enabling backend computerization for delivery of G2C services will ensure optimal leveraging and utilization of the core and support infrastructure such as Common Service Centres, Data Centre and State wide Area Network.

The objective of this Conformity Assessment Framework is to prepare the structured set of guidelines to facilitate the Third-Party Agency in assessing the conformance of the Digital platforms to the system requirements such as functional, performance, cyber security etc. and to extend the technical support to the developed solutions or similar applications in bringing them to an implementation stage at the earliest.

1.3 Coverage & Scope:

1) The scope for the Digital Platform Conformity Assessment is to be defined with reference to Digital India Programme.
2) The Digital India programme focuses on e-enabling the delivery of majority of citizen centric services.

3) Timelines: The programme generally will be implemented in two Phases:
   a) Stage I: Pre Go live conformance activities
   b) Stage II: Post Go live rolled out across the Nation/ State/ District subsequent to successful implementation in Stage 1 with activities like SLA, Process audit etc.
4) The first step in the implementation of the Stage I would be to identify the conformance activities as defined in RFP.
5) The end objective of the phases is to complete the conformance activities pre go live and post go live.

3rd Party Conformity Assessment Agency (3PCAA) shall be undertaking conformances assessment of digital platform applications/ System as per the requirements mentioned in the RFP of the project. The 3PCAA should also be involved right from the beginning so that they understand the requirements too. Their involvement should not be later than the FRS development stage. This certification should happen by the time the stage I is completed and before the Nation/ State-wide rollout.

2.0 Conformity Assessment:

Comprehensive assessment of the entire project to verify that various project components such as system, software application, network, infrastructure and processes are working in compliance to the project requirements as prescribed by the RFP document, along with the specifications, standards and other criteria stipulated for the project.

2.1 Conformity Assessment – Introduction:

1) Conformity assessment for the purpose of this engagement will include acceptance testing, assurance on conformance to standards & specifications with respect to application software, IT Hardware, the design and deployment of the front offices and IT upgradation of back offices as specified in the RFP and compliance to SLA's, process audit as detailed in the RFP.
2) The project covers various locations including DC, DR, front & back offices. A comprehensive list of all locations/ offices will provided in the RFP. For the purpose of compliance of the IT infrastructure and, the audit shall be for the full assets or for a representative set , as specified below:
   a) 100% of the IT assets in DC, DRC, HQs and Call Center;
   b) 100% of the IT infrastructure in Stage I front offices and 100% of the IT infrastructure in respective back offices;
   c) 100% of the IT infrastructure in the remaining front offices & in respective back offices, selected on sample basis in consultation with client.
3) The offices/ locations that would be audited in the stage I phase and the full roll out phase will also detailed in the RFP.
4) The 3rd Party Conformity Assessment Agency (3PCAA) will be involved with project from an early stage to ensure that
   a) The relevant guidelines/ standards are followed
   b) Large-scale modifications are avoided pursuant to assessment done after the system & application is fully developed and deployed.

2.2 Conformity Assessment - Purpose and Objectives:

The purpose of conformity assessment of the project is to verify that the Vision and objectives of the project, spelt out in the RFP are realized and the desired outcomes of the project are achieved. The TOR defines the scope of work for the 3rd Party Conformity Assessment Agency (3PCAA).

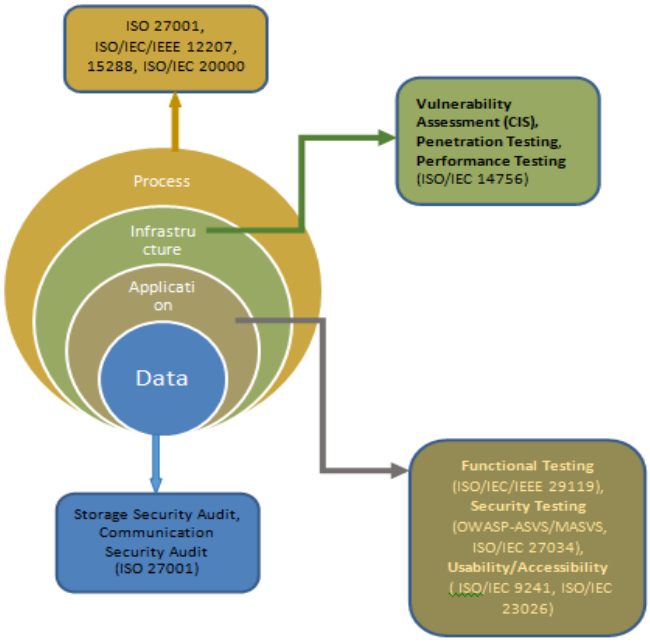
The key objectives of conformity assessment are to verify that:

a) The objectives and requirements prescribed in the project RFP are fulfilled;
b) The requirements, standards, specifications set out in the RFP are met;
c) The requirements, standards and specifications set out for those items whose standards are not specified in the RFP and any additional standards proposed by the Program Manager are met;
d) The RFP requirements have been implemented appropriately (i.e., Completely & Correctly).
e) The defects/ nonconformities are timely identified & are addressed before deployment.
f) Any additional item agreed between client, SP, and 3PCAA.

2.3 Conformity Assessment - Scope:

The conformity assessment shall cover various products and processes of the project including Software Application, Network, IT infrastructure at Data Center, Disaster Recovery Site and offices (front & back offices) for suitability and compliance to RFP/SRS.

The Quality & Security evaluation model consist of four layers namely, Data, Application, Infrastructure and Process depicted in below diagram:



The following components/ items will be taken up for conformity assessment as per the requirements specified in the RFP:

A) Review & audit of processes used by SP during development, operation & maintenance phases of the project covering life cycle, Security and IT Service Management processes.
B) Review of project/ product documents & records covering various project artifacts such as SRS, Design, Test Reports, etc.
C) Acceptance testing of software application for functional & non-functional requirements (application security, usability/accessibility, interoperability, performance etc.)
D) Code review of mobile apps for vulnerabilities
E) Testing & certification of Website quality as per national requirement.
F) Audit of IT including Data Center, Disaster Recovery Site, Network, Gateway, Front & Back Offices for compliance to architecture.
G) Audit of SLA measurement system & measurement of SLAs including critical parameters like performance, scalability, availability, etc.
H) Testing & Audit of system for Security including Vulnerability Assessment and Penetration Testing

The conformity assessment shall also address quality issues with emphasis on the Performance, Availability, Security, Usability, Interoperability, Manageability, as applicable according to the RFP.

The details of the project components/ items to be assessed are as under:-

A) Review & audit of processes used by SP during development, operation & maintenance phases of the project covering life cycle, Security and IT Service Management processes.

In general, the project sub-components/ sub-items covered in this category shall be as under. The specific requirements shall be taken from project RFP:

Project Sub-component/ Sub-items	
A1	Project Risk management process
A2	Strategic Control Systems put in place to facilitate exercise of respective roles and responsibilities of client and SP (see Note (a) below)
A3	Data migration process (see Note (b) below)
A4	Capacity management process
A5	Change Control process, Configuration Management & Release Management processes related to defect fixes and other changes (modifications/ enhancements) carried out in the development/ production environment (including OS, hardware/ application software changes, upgrades, etc.) & associated QA activities
A6	Internal QA processes including reviews, tests and audits used by SP
A7	Continuity & Availability Management process, Business Continuity Management process, Backup and storages processes including simulated business continuity/ disaster recovery drills (see Note (c) below)
A8	Support (Help Desk) function
A9	Incident & Problem management process
A10	Asset management process (see Note (d) below)
A11	Adequacy of user education/ training/ orientation
A12	Assessment of the Manageability of the system including, but not limited to, mandatory compliance to ITIL/ ITSM (see Note (e) below)
A13	Project processes as per applicability covering (Policy & Procedures): • System & Software Life Cycle Processes (Concept, Design, Development, Operational, Maintenance) • Information Security Management Processes (Management, Organizational, Operational, Technical) • IT Service Management Processes (Service Delivery & Support)

Note:

a) Strategic Control Systems

Project handles very sensitive functions & data. The sovereign control over the systems shall vest with the client. A framework for client to exercise such a control has been designed and prescribed in the RFP. The SP is required to design an appropriate system for giving effect to the Strategic Control Framework. The 3PAA shall review the Strategic Control Systems and related Policies & Procedures designed and developed by the SP to facilitate exercise of respective roles and responsibilities of client and SP as defined in the RFP and verify full conformance to the requirements of strategic control.

b) Data Migration Process

The 3PCAA shall perform the audit of Data Migration process prepared and implemented by SP for data migration. The 3PCAA shall also verify completeness and accuracy of migrated data on sample basis covering data from legacy database as well as that stored on any back-up media – especially with respect to creation of Master Database, checking of consistency, validation of key fields and data completeness.

c) Business Continuity/ Disaster Recovery drills

Conduct simulated business continuity/ disaster recovery drills under typical user loads of volume and mix (involving 100% switchover to DR site and contingency plans) and confirm compliance of Business Continuity Plans as well as the related documentation, with the requirements; repeat as required till set objectives of recovery and performance are reached.

d) Asset Management process:

- Procedures for acquisition/ procurement, installation/ alignment, usage and disposal/ termination of infrastructure components (including hardware components, software products/ licenses, services, etc. that may be applicable)
- Assessment of project requirements for managing procurements (including peak season needs)

e) Manageability of the System

The 3PCAA shall verify the manageability of the system and its supporting infrastructure using the Enterprise Management System (EMS) deployed by the SP. The manageability requirements such as remote monitoring, administration, configuration, inventory management, fault identification, fault analysis etc. shall have to be tested out, as per the terms defined in the RFP and agreed between client and SP. Fault identification tool should be such that it provides for exact identification of the component that has failed so that the recovery time is kept to the minimum.

3PCAA shall audit the systems, policies and procedures put in place and verify the mandatory compliance with ITIL/ ITSM.

B) Review of project/ product documents & records covering various artifacts such as SRS, Design, Test Reports, etc.

In general, the following project sub-components/ sub-items shall be covered under this category. The specific requirements shall be drawn from project RFP:

Project Documentation:

The 3PCAA shall review the project documents developed by SP including those relating to system requirements, system design, installation procedures, training and administration manuals, version management and others as specified in the RFP. 3PAA shall take care to assure conformance to the standard industry practices and the methodology proposed by the SP in their bid proposal.

Project Sub-component/ Sub-items	
B1	Review of the various project documentation, covering project deliverables, plans, reports & records
B2	Review of the Requirements Specification (RS), Software Requirements Specifications (SRS), User Manual (UM)
B3	Review of the Solution Design Architecture
B4	Review of the traceability matrix
B5	Review of the Internal QA including review, test & audit reports of SP

C) Acceptance testing of software application for functional & non-functional (Application Security, Usability, Interoperability and Performance) requirements

In general, the project sub-components/ sub-items covered under this category shall be as under. The specific requirements shall be taken from project RFP:

Functional Testing of Application Software:

The application software developed/ customized by SP shall be verified by the 3PCAA against the FRS and SRS signed-off between client and SP. Any gaps, identified as severe or critical in nature, shall be addressed by SP immediately prior to Go-live of the system. One of the key inputs for this testing shall be the traceability matrix to be developed by the SP. Apart from verifying the Traceability Matrix; 3PAA will develop its own test plan for validation of compliance of application software against the defined requirements.

3PAA will conduct the testing not only from the perspective of the software application development in conformity with the RFP, but especially from the usability of the various services and functionalities by the end users – employees of client, agents of the SP, citizens, and system administrators. User Interfaces provided for all these users will be critically examined and deficiencies and gaps pointed out and improvements suggested. Special emphasis may also be laid on the design of navigational convenience, uniformity of look and feel and aesthetics of the screens.

Application Security Testing

The test is conducted to unearth various application security vulnerabilities, weaknesses and concerns related to Data /Input Validation, Authentication, Authorization /Access Control, Session Management, Error Handling,

Use of Cryptography, etc. Typical issues which may be discovered in an application security testing include Cross-site scripting, Broken ACLs/Weak passwords, Weak session management, Buffer overflows, Forceful browsing, Form/hidden field manipulation, Command injection, SQL injection, Cookie poisoning, Insecure use of cryptography,, Mis-configurations, Well-known platform vulnerabilities, Errors triggering sensitive information leak etc. OWASP (Open Web Application Security Project) guidelines are used for the testing.

Application Usability Testing

Usability testing usually involves systematic observation under controlled conditions to determine how well people can use the product. Digital Platform system is used by users of different levels of computer knowledge. User expectation varies with different types of user. Usability testing will ensure that the all types of users are comfortable to use the system. This shall be done by using defined international standards which recommend extensive user interaction and analysis of user behaviour for a defined task.

Application Interoperability and Compatibility Testing

Interoperability Testing shall be done to check if the software can co-exist and interchange data with other supporting software in the system. Compatibility testing shall check if the software runs on different types of operating systems and other hardware/software/interface according to customer requirements

Performance Testing of the System

Performance testing of the Digital Platform System shall be done to ensure that system is capable of handling defined user as well as transactional load. The performance testing of the Digital Platform System essentially means measuring the response time of the system for defined scenarios. While measuring the response time it is important to record the resource (CPU, Memory, etc.) utilization. The capacity of the Digital Platform System should be checked by systematically increasing the load on the system till performance degradation or system crash is encountered. Also the manner/ trend in which performance changes with load will determine the scalability of the Digital Platform System.

Application Code review

The code review (i.e., static analysis) of the software application source code shall be carried out using tool and measure metrics such as lines of Code, Code Complexity, Fan-in & fan-out, Application Call Graph, Dead Codes, Rule Violation, Memory leaks etc. It is also recommended to perform walk through of the source code with code developer to verify the logics and algorithms used for correctness and optimization. Special focus should be given to identify any unwanted functions (not required by the Digital Platform Software Application), as these 'not to have functionalities' can be potential security threats.

Project Sub-component/ Sub-items	
C1	Functional Testing of the Application Software developed by the SP
C2	Application Security Testing of the Application Software developed by the SP
C3	Usability of the Application Software
C4	Application Interoperability and Compatibility Testing (Interfaces with other applications like establishment application, payment gateways, banks, Accounts, etc.)
C5	Performance Testing of the System
C6	Adherence to applicable Coding standards as per RFP

D) Code review of mobile apps for vulnerabilities

Review of code for Mobile applications for vulnerabilities related to security. The SP shall submit non-obfuscated codes for android / IOS Mobile Apps.

System Sub-component/ Sub-items

D1	Scanning of the non-obfuscated code for vulnerabilities.
D2	Review of Tool report, if any for false positive

E) Testing & certification of Website quality as per national requirement.

In general, the following project sub-components/ sub-items shall be covered under this category. The specific requirements shall be drawn from project RFP:

	Project Sub-component/ Sub-items
E1	Website quality for functionality, performance, security, usability, accessibility and content management system.
E2	Compliance to Guidelines For Indian Government Websites Quality of Content, Design, Development, Website hosting, Website Promotion and website management.

F) Audit of IT Infrastructure including Data Centre, Disaster Recovery Site, Network, Gateway, and Front & Back Office for compliance to architecture:

IT infrastructure audit shall cover DC, DR, gateway, Network, Front & Back offices. Audit of offices will be done on random sampling basis. The focus of the audit shall be on IT infrastructure.
In general, the project sub-components/ sub-items covered under this category shall be as under. The specific requirements shall be taken from project RFP:

Infrastructure Compliance Audit

3PAA shall perform the Infrastructure Compliance audit to verify the conformity of the Infrastructure supplied/ deployed by the SP against the requirements and specifications provided in the RFP and/or as proposed in the proposal submitted by SP. This includes

- Compliance of the deployed architecture against the solution architecture.
- Verification of the specifications of the hardware, networking equipment and system software w.r.t the design documents.
- Configuration settings and load testing of the IT infrastructure
- Assessing the scalability of the system, especially the servers and the network equipment.
- Verification of the IT infrastructure at the front & back offices on sample basis and 100% at the DC & DR.
- Verification of the compliance with the requirements of the Gateway, in terms of separation of the front-end from backend and interoperability.

	Project Sub-component/ Sub-items
F1	Review & audit of deployed IT infrastructure for compliance & adherence to the Architecture and standards specified in the RFP/SRS.
F2	Verification of IT Infrastructure for compliance
F3	Performance & Availability of IT infrastructure including Network
F4	Security of infrastructure covering: o Adequacy of Security Policy & Requirements o Implementation & effectiveness of applicable security controls (Management, Operation & Technical)

G) Audit of SLA measurement system & Measurement of SLAs including critical parameters like performance, scalability, availability, etc.

In general, the following project sub-components/ sub-items shall be covered under this category. The specific requirements shall be drawn from project RFP:

SLA Management System

SLA Management is the heart of the system during the O&M phase. The payments to the SP are dependent on the performance against the SLA. To this extent the SLA Management system of the Project should be accurate, reliable and trustworthy. As per the RFP, the SP shall design and implement the SLA Management System which includes a comprehensive and robust tool required to monitor all the performance indicators listed under SLA of the RFP.

It is the responsibility of the 3PAA to ensure that the design, deployment and management of the SLA Management System fulfill this requirement. The 3PCAA shall verify the accuracy, reliability and completeness of the information captured by the SLA monitoring system implemented by the SP. The system shall be capable to calculate the billable transactions logged and transaction-based payout due to SP in a defined period as per specifications provided in the RFP.

Performance

Performance is another key requirement for system and 3PCAA shall review the mechanism put in place for achieving the desired performance of the deployed solution as per the SLA and other related terms defined in the RFP and agreed between client and SP. The performance testing shall also include verification of scalability provisioned in the system for catering to the requirements of application volume growth in future.

The response times of the system for accessing various functionalities and services shall be critically examined w.r.t the specifications of the RFP while conducting the performance review.

	Project Sub-component/ Sub-items
G1	Review & audit of the SLA Management System, methodology and tools deployed for SLA measurement for verification of adequacy & suitability including of data probes for data collection, locations, data collection, SLAs computations and reporting
G2	Compliance with the SLA metrics as defined in the RFP
G3	Audit & measurement of system Performance of the system, especially w.r.t peak load conditions and scalability
G4	Audit & measurement of system Availability
G5	Measurement of SLAs using industry standard tool to compare SLAs measurement results obtained with those reported by SP.

H) Testing & Audit of system for Security including Vulnerability Assessment and Penetration Testing

In general, the project sub-components/ sub-items covered under this category shall be as under. The specific requirements shall be taken from project RFP:

Security Testing & Audit

The software & system developed/ customized for system shall be audited by the 3PCAA from a security & controls perspective. 3PCAA shall also review & audit the Security Policy laid and the Operational Procedure Documents designed by the SP on ISMS and shall cover entire ecosystem including DC, DRC, Gateway, front offices, back offices etc. Such audit shall also include the IT infrastructure and Network deployed for system.

The security testing & audit shall subject the system for the following key activities:

- Audit of Network, Server and Application security mechanisms
- Assessment of authentication mechanism provided in the application /components/ modules
- Assessment of data encryption mechanisms implemented for the solution
- Assessment of data access privileges
- Assessment of data back-up & archival mechanisms, retention periods and restoration mechanism
- Server and Application security features incorporated

- System, organizational as well as IT-enabled, for management of Digital Signature Certificates for both Client and SP personnel
- Security culture nurtured and practiced by Client and SP in the ecosystem
- Any other aspect relevant to system as per the Security policy defined

Project Sub-component/ Sub-items	
H1	Architecture Review
H2	Configuration and monitoring of firewall, intrusion detection and prevention system, switches, routers etc. Testing & Audit of the information Security system including, vulnerability assessment
H3	Penetration Testing

2.4 Conformity Assessment – Applicable References:

The following documents will be used as sources of information for the conformity assessment plan and preparation:

- Request For Proposal (RFP)
- Terms of Reference (TOR) for conformity assessment
- Conformity Assessment Framework Document
- Applicable Standards and Guidelines (National Guidelines)
- Products & process documents and related records of the project
- System logs & records of the project
- Any other Related Documents
- Standards Applicable:
  - ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements
  - ISO/IEC 27033 — IT network security
  - ISO/IEC/ IEEE 29148 Systems and software engineering — Life cycle processes — Requirements engineering
  - ISO/IEC/ IEEE 42010 Systems and software engineering — Architecture description
  - ISO/IEC/ IEEE 26512 Systems and software engineering — Requirements for acquirers and suppliers of user documentation
  - ISO/IEC/ IEEE 29119-1 Software and systems engineering — Software testing — Part 1: Concepts and definitions
  - ISO/IEC/ IEEE 29119-2 Software and systems engineering — Software testing — Part 2: Test processes
  - ISO/IEC/ IEEE 29119-3 Software and systems engineering — Software testing — Part 3: Test documentation
  - ISO/IEC/ IEEE 29119-4 Software and systems engineering — Software testing — Part 4: Test techniques
  - ISO/IEC 27034 — Application security
  - ISO/IEC/IEEE 12207 & 15288 , CMMI
  - OWASP Mobile Application Security Verification Standard (MASVS)
  - OWASP Application Security Verification Standard 4.0

2.5 Conformity Assessment - Stage:

The conformity assessment is required to be carried out in 2 stage specified below:

1) **Stage-I** - Pre-Go-Live assessment of the Stage I and statement-of-compliance of the stage I sites.
2) **Stage-II** - Pre-Go-Live assessment of the complete Rollout of project and statement-of-compliance of the Rollout.

2.6 Conformity Assessment - Approach & Methodology:

Conformity assessment shall be carried out through review, testing & audit of various project components such as Software Application, IT Infrastructure, Solution Architecture, IT Operations, Service Level Agreements, etc. covering Data Center, Disaster Recovery Site, Network and offices (front & back offices) for compliance to RFP. The conformity assessment activities shall be undertaken under simulated conditions and/ or production environment as required.

Conformity Assessment shall be carried out by independent Third Party Conformity Assessment Agency (3PCAA), covering project locations where project has been deployed and is operational. Audit will be done on the sampling basis using vertical and horizontal audit strategies to verify items (covering various products & processes of the project and related documents & records) as mentioned in the scope for:

2.6.1 Conformity Assessment - Steps:

Steps of Conformity Assessment shall be as follows:

1. Planning & Preparation
2. Conduction
3. Reporting
4. Corrective action by SP on the nonconformities/ observations reported
5. Verification and closure of nonconformities / observations

2.6.2 Conformity Assessment - Inputs:

Following inputs shall be needed by the 3PCAA to carryout audit:

- Products & process documents and related records
- Access to system, system logs, reports & related information

Specific inputs required for assessment of various project components/ items are given in Annexure ‘A’ to ‘H’.

2.6.3 Conformity Assessment - Activities & Tasks:

The key conformity assessment activities comprise of reviews, testing & audit of various products & processes of the project. These activities will be performed on the system including hardware, software, Network & IT infrastructure and processes, various documents and associated information of the system. The key aims of review, testing & audit are as follows:

Review shall be performed for Documentation covering Policies, Procedures, and System & Software. Review shall be undertaken for:

- Verification of software documents for adequacy of description & details as per RFP
- Completeness, Correctness, Clarity & Consistency of documents
- Traceability of documents to previous and later phases of the project.
- Compliance with Technical Standards
- Adherence to Document Control practices and Applicable Standards
- Verification of internal QA - review & test records of SP

Review defects shall be assigned severity as follows:

Review Defect Severity	Description
Urgent	Absence of the document, i.e., document not available (missing)
High	Critical information/ contents of the document completely or partially missing/ wrong/ misleading. The defect/ deviation is given high attention to resolve on priority
Medium	Significant defect/ deviation to comply with documentation requirement

Low	Single observed isolated lapse in the document. A minor problem having negligible effect on document quality & warranting attention
None	None of the above, or the defect/ deviation is addressed to enhance document quality

Testing shall be undertaken for Software, Hardware, Network, SLAs, etc. Testing shall be performed to:

- Verify that all functional requirements are implemented as per specified requirements in the RFP
- Verify that the non-functional requirements (i.e., software characteristics) such as performance, security, interoperability, usability, etc. as specified by RFP have been fulfilled.
- Identify defects & ensure that they are addressed before system/ software is deployed.

Test defects identified shall be classified in terms of severity as follows:

Test 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.

Audit shall cover project processes (e.g., QMS, ISMS, ITSM), systems, infrastructure including CSC, Network, DC, DR, Gateway, front & back offices, etc. Audit shall be carried out to verify:

- Adequacy of defined processes as per applicable Standards
- Implementation of defined processes in the project
- Effectiveness of the implemented processes in meeting the desired objectives

Audit nonconformities shall be classified for severity as follows:

Audit Nonconformity Severity	Description
Urgent	Absence or total breakdown of process requirement
High	Critical requirement is completely or partially missing/ wrong/ misleading. The defect/ deviation is given high attention to resolve on priority
Medium	Significant failure to comply with specified process requirement
Low	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 defect/ deviation is addressed to enhance document quality

In general, following common activities shall be involved in review, testing & audit:

- Study and understand the items and its requirements for review/ test/ audit.
- Prepare checklists & test cases
- Conduct review/ test/ audit
- Record observations/ logs
- Analyze & identify nonconformities/ defects
- Prepare review/ test/ audit report

Activities & tasks to be performed by the conformity assessment agency are given in Annexure ‘A’ to ‘H’.

For this 3PCAA team shall be provided with access to system, various documents and associated information. 3PCAA team shall also be allowed to 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.

2.6.4 Conformity Assessment Outputs:

The following outputs shall be the produced:

- Conformity Assessment Plan
- Checklists/ Questionnaires
- Recordings/ Logs
- Conformity Assessment Report
- Nonconformity/ Observation Closure Report

Specific outputs produced by assessment of various project components/ items are given in Annexure 'A' to 'H'.

2.6.5 Conformity Assessment - Criteria:

The criteria for compliance of the project component or the complete project to RFP requirements are given at annexure-1. Client has to define the acceptance criteria base on compliance achieved.

- The audit items shall comply with the project requirements.
- The reported nonconformities/ observations shall be closed satisfactorily.

2.7 Conformity Assessment - Deliverables:

The followings shall be submitted by the audit agency to the client:

- Conformity Assessment Plan
- Conformity Assessment Report
- Nonconformity/ Observation Closure Report

Deliverables of assessment of various project components/ items are given in Annexure 'A' to 'H'.

3.0 Responsibilities:

The responsibilities of various parties involved are as under:

3.1 Client:

The client/ user of the system shall support the 3PCAA team in the following activities:

- Act as interface between audit agency & operator
- Provide domain expertise
- Assistance during audit

3.2 Implementation Partner/ Solution Provider (SP):

Implementation Partner/ Solution Provider provide development, operation and maintenance services to project and shall be responsible for followings:

- Making the required audit inputs available to audit agency
- Provide access to the system
- Initiate timely action to fix the nonconformities/ observations reported
- Demonstrate the satisfactory closures of the reported nonconformities/ observations

3.3 Conformity Assessment Agency (3PCAA):

Third Party Conformity Assessment Agency (3PCAA) shall be responsible for followings:

- Overall management and planning the audit
- Conduction of the audit and feedback to operator for corrective action

- Submit audit deliverables to client

Annexure – 1: Criteria for Compliance

1. RFP Completeness:

Review/ Test/ Audit the project component/ item and evaluate the associated RFP requirements for completeness of implementation and assign percentage completeness. Depending upon the completeness, assign Requirement Completeness Status and Requirement Completeness Score to RFP requirement using following table:

Basis of Assigning Requirement Completeness Score		
Requirements Completeness Status	**Completeness (%)**	**Requirement Completeness Score**
Fully Implemented	**100%**	**1.00**
Largely Implemented	**75% to <100%**	**0.75**
Partially Implemented	**50% to <75%**	**0.50**
Minimally Implemented	**40% to <50%**	**0.25**
Not Implemented	**<40%**	**0**
Deferred/ To be Implemented in future	**NA, if Deferred by user, otherwise 0%**	**NA, if Deferred by user, otherwise 0**

2. RFP Correctness:

Review/ Test/ Audit the project component/ item and based on the deviation (i.e., defect/ nonconformity severity) found evaluate the associated RFP requirements for correct implementation and assign percentage deviation. Depending upon the deviation, assign Requirement Correctness Status and Requirement Correctness Score to RFP requirement using following table:

Basis of Assigning Requirement Correctness Score			
Requirements Correctness Status	**Defect/ NC Severity**	**Deviation (%)**	**Requirement Correctness Score**
No Deviation	**None**	**<40%**	**1.00**
Minimal Deviation	**Low**	**40% to <50%**	**0.75**
Partial Deviation	**Medium**	**50% to <75%**	**0.50**
Large Deviation	**High**	**75% to <100%**	**0.25**
Full Deviation	**Urgent**	**100%**	**0**
Could not be Tested	**NA**	**NA, if deferred/ waived off by user, otherwise 100%**	**NA, if deferred by user, otherwise 0**

Calculate, Requirement Compliance for RFP requirements using following formula:

Requirement Compliance = Requirement Completeness * Requirement Correctness

For the project component/item to be evaluated, prepare the following table:

Reference Document: RFP/ Contract/ Project Document (E.g., Software, Architecture, SRS/ UM, etc.)

Sr. No.	RFP/ Contract Requirements	Project Document Reference	Requirements Status (Score)		Requirement Compliance	Comments
			Completeness	Correctness		
1.						
2.						
3.						
4.						

5.						

Compute the followings,

RFP Completeness (%) = ∑ Requirement Completeness (%)/ Number of RFP Requirements

RFP Correctness (%) = ∑ Requirement Correctness (%)/ Number of RFP Requirements

RFP Compliance (%) = ∑ Requirement Compliance (%)/ Number of RFP Requirements

Use following criteria to assign RFP Compliance/ Quality Rating:

RFP Compliance (%)	RFP Compliance Score	RFP Implementation Coverage	
		RFP Compliance	Quality Rating
95% and Above	1.00	Fully Satisfied	Excellent
75% to <95%	0.75	Largely Satisfied	Very Good
50% to <75%	0.50	Partially Satisfied	Good
40% to <50%	0.25	Minimally Satisfied	Acceptable
<40%	0	Not Satisfied (Needs Improvement)	Not Acceptable (Needs Improvement)

Acceptance Criteria:

The criteria for acceptance shall be defined by the client for the followings:

- The RFP implementation coverage shall be Fully/ Largely satisfied (client to define)
- All the critical RFP requirements (client to define) shall be fully implemented.
- No Urgent & High severity deviation/ defect shall remain open.
- Unless specified, all the requirements shall be considered to be equally important
- Implementation coverage shall be evaluated RPF Vs. software application.

The condition for acceptance and issue of Statement of Conformity is successful completion & compliance of the pilot & rollout phases of the project (i.e., RFP Compliance – Largely/ Fully Satisfied or Quality Rating – Excellent/ Very Good) and all the critical requirements are fully implemented and defects (Urgent & High severity) are closed.

Annexure 'A' – Conformity Assessment framework Details

"Review & audit of processes used by SP during development, operation & maintenance phases of the project covering life cycle, Security and IT Service Management processes"

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
A1	Project Risk management process	• Risk Management policy and procedural documents • Risk Management plan • Associated Records	• Review of Risk Management policy, procedural & plan documents • Audit of Risk Management process	• Nonconformities and observations in Risk Management process	
A2	Strategic Control Systems put in place to facilitate exercise of respective roles and responsibilities of client and SP	• Strategic Control Systems policy and procedural documents • Associated Records	• Review of Strategic Control Systems policy, procedural & plan documents • Audit of Strategic Control Systems	• Nonconformities and observations in Strategic Control Systems	
A3	Data Migration process	• Data Migration policy and procedural documents • Data Migration plan • Associated Records	• Review of Data Migration policy, procedural & plan documents • Audit of Data Migration process	• Nonconformities and observations in Data Migration process	
A4	Capacity Management process	• Capacity Management policy and procedural documents • Capacity Management plan • Associated Records	• Review of Capacity Management policy, procedural & plan documents • Audit of Capacity Management process	• Nonconformities and observations in Capacity Management process	
A5	Change Control process, Configuration Management & Release Management processes related to defect fixes and other changes (modifications/ enhancements) carried out in the development/ production environment (including OS, hardware/ application software changes, upgrades, etc.) & associated QA activities	• Change Control, Configuration Management & Release Management policy and procedural documents • Management plans • Associated Records	• Review of policy, procedural & plan documents • Audit of Change Control, Configuration Management & Release Management processes & associated QA activities	• Nonconformities and observations in Change Control, Configuration Management & Release Management process	
A6	Internal QA processes including reviews, tests and audits used by SP	• Internal QA policy and procedural documents • Internal QA plan • Associated records	• Review of Internal QA policy, procedural & plan documents • Audit of Internal QA	• Nonconformities and observations in internal QA	Refer-B5

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
			processes	processes	
A7	Continuity & Availability Management process, Business Continuity Management process, Backup and storages processes including simulated business continuity/ disaster recovery drills	• Policy and procedural documents • Management plans • Associated Records	• Review of policy, procedural & plan documents • Audit of process • DR drill and post drill tests to verify success	• Nonconformities and observations in the process	Refer-G4
A8	Support (Help Desk) function	• Support (Help Desk) policy and procedural documents • Associated Records	• Review of Support (Help Desk) policy and procedural documents • Audit of Support (Help Desk)	• Nonconformities and observations in Support (Help Desk)	
A9	Incident & Problem Management process	• Incident & Problem Management policy and procedural documents • Associated Records	• Review of Incident & Problem Management policy and procedural documents • Audit of Incident & Problem Management process	• Nonconformities and observations in Incident & Problem Management process	
A10	Asset management process	• Asset Management policy and procedural documents • Asset lifecycle • Asset Management Plan • Asset records & logs	• Review & asset management policy, procedural & plan documents Audit of asset management process	• Nonconformities and observations in asset management process	
A11	Adequacy of user education/ training/ orientation	• User education/ orientation plan • User manual & User training kit • Associated Records	• Review of User education/ orientation plan • Audit of User education/ orientation	• Nonconformities and observations in user education/ orientation process	
A12	Assessment of the Manageability of the system including, but not limited to, mandatory compliance to ITIL/ ITSM (see Note (e) below)	• Applicable ITIL/ ITSM processes • Policy, procedural and plan documents • Associated Records	• Review of policy, procedural & plan documents • Audit of applicable ITIL/ ITSM processes	• Nonconformities and observations in applicable ITIL/ ITSM processes	Refer-A13
A13	Project processes as per applicability covering (Policy & Procedures): • System & Software Life Cycle Processes (Concept, Design, Development, Operational,	• Applicable processes • Policy, procedural and plan documents • Associated Records	• Review of policy, procedural & plan documents • Audit of applicable processes	• Nonconformities and observations in applicable processes	

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
	Maintenance) • Information Security Management Processes (Management, Organizational, Operational, Technical) • IT Service Management Processes (Service Delivery & Support)				

"Review of project/ product documents & records covering various artifacts such as SRS, Design, Test Reports, etc."

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
B1	Review of the various project documentation, covering project deliverables, plans, reports & records	• Project Documents • Project Plans including associated plans & Records	• Review to verify adequacy, completeness, correctness, consistency, traceability & document control aspects of project documents	• Defects and observations in project documents	
B2	Review of the Requirements Specification (RS), Software Requirements Specifications (SRS) & User Manual (UM)	• Requirements Specification (RS) document • Software Requirements Specifications (SRS) document • User Manual (UM)	• Review to verify adequacy, completeness, correctness, consistency, traceability & document control aspects of requirements documents	• Defects and observations in RS, SRS & UM Documents	
B3	Review of the Solution Design Architecture	• Solution Architecture Document	• Review to verify adequacy, completeness, correctness, consistency, traceability & document control aspects of solution architecture	• Defects and observations in Architecture Document	
B4	Review of the traceability matrix	• Traceability matrix document	• Verify completeness & correctness of traceability matrix	• Defects and observations in traceability matrix	
B5	Review of the Internal QA documents including review, test & audit reports of SP	• Internal QA documents including review, test & audit reports of SP	• Verify adequacy and appropriateness of internal QA documents	• Defects and observations in internal QA documents	Refer-A6

"Acceptance testing of software application for functional & non-functional requirements"

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
C1	Functional Testing of the Application Software developed by the SP	• Software Requirements Specifications • User Manual	• Testing (Black box) to verify requirements and identify defects	• Defect Report • Test Report	
C2	Application Security Testing of the Application Software developed by the SP	• Adequacy of Security Policy & Requirements • Role wise Application Access Matrix	• Automatic Scanning of the Application • Manual Testing	• Security Test Report	Refer F4
C3	Usability of the Application Software	• Types of user • Filled Questionnaire	• Testing	• Usability Test Report	
C4	Application Interoperability and Compatibility Testing (Interfaces with other applications like establishment application, payment gateways, banks, Accounts, etc.)	• Interface specifications with external applications • Server logs	• Testing of system/ software interfaces	• Defects and observations on interfaces with other applications	
C5	Performance Testing of the System	• Performance & Load workflow • Server logs	• Performance Testing	• Performance Test Report	Refer F3
C6	Adherence to applicable Coding standards as per RFP	• Source Code of application software • Coding guidelines	• Review and analysis for adherence to coding standards	• Review Report	

Annexure 'D' – Conformity Assessment Details

" Code review of mobile apps for vulnerabilities"

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
D1	Scanning of the non-obfuscated code for vulnerabilities	• Non-obfuscated code	• Review	• Defect Report • Test Report	
D2	Review of Tool report, if any for false positive	• Tool report of code	• Compliance verification as per checklist	• Compliance Report	

Annexure 'E' – Conformity Assessment Details

"Testing & certification of Website quality as per national requirement"

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
E1	Website quality testing for functionality, performance, security, usability, accessibility and content management system.	• Website Requirements Document • CMS Document	• Website testing	• Defect Report • Test Report	
E2	Compliance to Guidelines For Indian Government Websites, January 2009 Quality of Content, Design, Development, Website hosting, Website Promotion and website management.	• Website	• Compliance verification as per checklist	• Compliance Report	

Note:

In case of web-based software application, website testing shall be included in Software application testing.

Annexure 'F' – Conformity Assessment Details

"Audit of IT Infrastructure"

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
F1	Review & audit of deployed IT infrastructure for compliance & adherence to the Architecture and standards specified in the RFP/SRS.	• List of IT infrastructure	• Review	• Review Report	
F2	Verification of IT Infrastructure for compliance	• Review Report	• Audit	• Audit Report	
F3	Performance & Availability of IT infrastructure including Network	• Application Workflow	• Performance Testing	• Performance Testing Report	Refer C5
F4	Security of infrastructure covering: • Adequacy of Security Policy & Requirements • Implementation & effectiveness of applicable security controls (Management, Operation & Technical)	Security Document	• Security testing	• Security Testing Report	Refer C2

Annexure 'G' – Conformity Assessment Details

"Audit of SLA measurement system & Measurement of SLAs including critical parameters like performance, scalability, availability, etc."

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
G1	Review & audit of the SLA Management System, methodology and tools deployed for SLA measurement for verification of adequacy & suitability including of data probes for data collection, locations, data collection, SLAs computations and reporting	SLA Measurement Methodology document	Audit	SLA Report	
G2	Compliance with the SLA metrics as defined in the RFP	SLA Measurement Methodology document	Audit	SLA Report	
G3	Audit & measurement of system Performance of the system, especially w.r.t peak load conditions and scalability	SLA Measurement Methodology document	Audit	SLA Report	
G4	Audit & measurement of system Availability	SLA Measurement Methodology document	Audit	SLA Report	
G5	Measurement of SLAs using industry standard tool to compare SLAs measurement results obtained with those reported by SP.	SLA Measurement Methodology document	Audit	SLA Report	

Annexure 'H' – Conformity Assessment Details

"Testing & Audit of system for Security including Vulnerability Assessment and Penetration Testing"

Sr. No.	Project Sub-component/ Sub-items	Inputs Required	Activities & Tasks	Outputs Produced	Remarks
H1	Architecture Review	Network diagram of DC & DR along with description stating network devices and network Security Infrastructure	Review and Audit	Architecture Review/ Audit Report	
H2	Configuration and monitoring of firewall, intrusion detection and prevention system, switches, routers etc. Testing & Audit of the information Security system including, vulnerability assessment,	List of Device type along with Server/ Device Hostname, IP Address, Role and OS	Assessment and Testing	Vulnerability Assessment Report	
H3	Penetration Testing	List of IPs	Assessment and Testing	Penetration Testing Report	