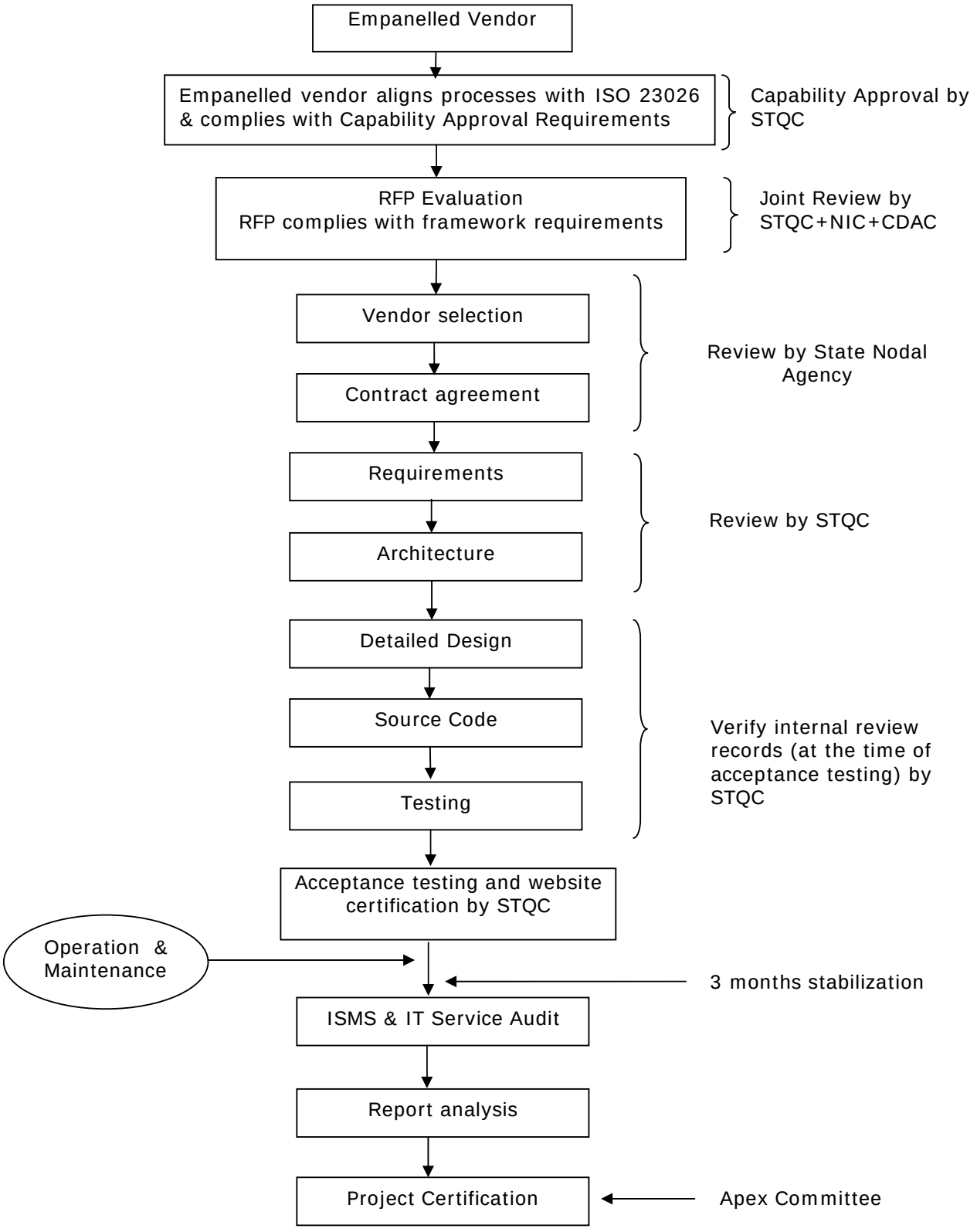
11. State Portal Conformity Assessment Requirement

The purpose of this Conformity Assessment Requirement is to ensure that all State Portal implementations would adhere to defined standards, recommendations, best practices. It also brings the consistency between different State Portals so as to provide common user experience to the citizen as well as to interoperate with each other for content/service sharing.

Objective of Conformity Assessment Requirement would be to ensure compliance of State Portal with:

a. Functional and architectural requirements of State Portal
b. State portal reference architecture
c. State portal framework
d. Policies and standards of State government
e. Process for development, management and sustenance of State Portal

The flow diagram below depicts the various conformity assessment activities:


Empanelled Vendor
Empanelled vendor aligns processes with ISO 23026 & complies with Capability Approval Requirements
Capability Approval by STQC
RFP Evaluation
RFP complies with framework requirements
Joint Review by STQC+NIC+CDAC
Vendor selection
Contract agreement
Review by State Nodal Agency
Requirements
Architecture
Review by STQC
Detailed Design
Source Code
Testing
Verify internal review records (at the time of acceptance testing) by STQC
Acceptance testing and website certification by STQC
Operation & Maintenance
3 months stabilization
ISMS & IT Service Audit
Report analysis
Project Certification
Apex Committee

11.1. Constituents of Conformity Assessment Requirement

State Portal Conformity Assessment Requirement consists of following

- Compliance checkpoints: Defines when compliance verification need to be performed and what artefacts need to be verified.
- Compliance process: Provides process to be used for performing compliance verification
- Compliance checklist: Provides detailed list of items to verified as part of compliance verification.

11.2. Compliance Checkpoints

Following table provides compliance checkpoints and input artefacts for each of the processes.

Stage	Phase	Deliverables/ Artefacts	Compliance Checkpoints	Responsibility
Acquisition	RFP Preparation	Business Requirements	Review	State Nodal Agency
		Detailed Project Report (DPR)	Review	State Nodal Agency
		RFP Document	Joint Review	Technical Review Team
	Vendor Selection	Bid Evaluation Report	Review	State Nodal Agency
	Contract Agreement	Contract Agreement Document	Review	State Nodal Agency
	Contract Monitoring	Monitoring Reports	Monitor & Review	State Nodal Agency
Design and development	Requirements Analysis	Requirements Specifications	Review	STQC
		Requirements Traceability Document	Review	STQC
	Architecture Design	Architecture Design Document	Review	STQC
		Traceability Document	Review	STQC
	Detailed Design	Detailed Design Document	Verify internal review records (at the time of acceptance testing)	STQC
		Traceability Document	Verify internal review records (at the time of acceptance testing)	STQC
	Coding	Source Code	Verify internal review records (at the time of acceptance testing)	STQC
		Traceability Document	Verify internal review records (at the time of acceptance testing)	STQC
	Testing	Test Plan	Verify internal review records (at the time of acceptance testing)	STQC
		Test Cases	Verify internal review records (at the time of acceptance testing)	STQC
		Traceability Document	Verify internal review records (at the time of	STQC

Stage	Phase	Deliverables/ Artefacts	Compliance Checkpoints	Responsibility
			acceptance testing)	
		Test Reports	Verify internal review records (at the time of acceptance testing)	STQC
Solution Ready for Acceptance Testing by Third Party (STQC)				
Acceptance	Acceptance Testing	Acceptance Test Plan Acceptance Test Report	Review	State Nodal Agency
		Developed Solution	Third Party Testing of developed solution	STQC shall undertake Acceptance Testing by carrying out Test Planning, Test Execution and submit Acceptance Test Report.
	Deployment	Deployment Plan	Review	STQC
		Deployed Solution	Third Party Audit of deployed architecture	STQC shall undertake audit and submit report for audit of: • Solution as per design architecture • IT Infrastructure as per BoM
Based on the satisfactory compliance with the criteria, STQC will issue the following: 1. Website Quality Certificate (Quality Level 1), 2. Conformity Assessment Reports for SPF Recommendation for approval of state portal will be done by steering committee. Upon the recommendation of the steering committee, final approval/ certification will be granted by the apex committee.				
Operation and Maintenance	User Training	Training Plan and Records	Monitor & Review	State Nodal Agency
	User Support	Reports, Tickets	Monitor & Review	State Nodal Agency
	Performance Monitoring	Performance Reports	Monitor & Review	State Nodal Agency
	Maintenance	Maintenance Plan	Verify Internal Review Records	STQC
		Maintenance Records	Monitor & Review	State Nodal Agency
Service Delivery	Information Security Management Processes	Security Policy Document	Third Party Audit	STQC
		Asset Management Plan & Procedure	Third Party Audit	STQC
		Risk Management Plan & Procedure	Third Party Audit	STQC
		Human Resources Security Plan & Procedure	Third Party Audit	STQC
		Physical & Environmental Security Plan & Procedure	Third Party Audit	STQC
		Communications & Operations Management Plan & Procedure	Third Party Audit	STQC
		Access Control Plan & Procedure	Third Party Audit	STQC
		Information Systems Acquisition, Development & Maintenance Plan & Procedure	Third Party Audit	STQC
		Information Security Incident Management Plan & Procedure	Third Party Audit	STQC
		Business Continuity Management Plan & Procedure	Third Party Audit	STQC
	IT Service	• Policy Document	Third Party Audit	STQC

Stage	Phase	Deliverables/ Artefacts	Compliance Checkpoints	Responsibility
	Management Processes	Plan & Procedure for Service Delivery Processes: • Service Level Management • Service Reporting • Service Continuity & Availability Management • Budgeting & Accounting for IT Services • Capacity Management • Information Security Management	Third Party Audit	STQC
		Plan & Procedure for Relationship Processes: • Business Relationship Management • Supplier Management	Third Party Audit	STQC
		Plan & Procedure for Resolution Processes: • Incident Management • Problem Management	Third Party Audit	STQC
		Plan & Procedure for Control Processes: • Configuration Management • Change Management	Third Party Audit	STQC
		Plan & Procedure for Release Process: • Release Management Process	Third Party Audit	STQC

11.3. Compliance Process

Audit, Compliance verification or validation is essential to achieving the objectives, ensuring development and maintenance of State Portal. Compliance process would be used to verify compliance with respect to defined standards, guidelines and best practices.

Following table provides various activities to be performed by author, reviewer and approver as part of compliance process.

Steps	Author	Reviewer	Approver
1.	Prepare artefact		
2.		Formulate review team	
3.	Plan for review meeting		
4.	Circulate artefacts to review team		
5.	Conduct briefing session on artefacts		
6.		Review artefacts	
7.		Mail review comments to author	
8.	Prepare response to review comments		
9.	Discuss review comments, response to review comments and finalize closure actions		
10.	Circulate review record with		

	proposed changes		
11.	Update artefacts incorporating review comments as per agreed closure actions		
12.	Circulate updated artefacts		
13.		Check incorporated review comments	
14.		Prepare compliance report	
15.	Send artefact to approver		
16.	Conduct approval meeting		
17.			Approve artefacts
18.			
19.	Release artefact		

11.4. Compliance Checklist Usage Guidelines

"Compliance Checklist" would be used by "Technical review team" to perform compliance assessment of work products. This checklist should be used for compliance verification during state portal implementation process and thereafter to monitor the performance of State Portal. Compliance verification should be performed whenever artefacts are created or modified.

Following sub-sections gives list of artefacts which need to be verified during compliance audits. These artefacts are explained in the "Governance Framework" section of State Portal Framework document and below information is copied here for convenience. Compliance checklist refers these artefacts along with each compliance item.

Note: Complete list of deliverables is provided in the "Governance Framework" section. As a ready reference deliverables related to "State Portal Implementation" and "Performance Monitoring and Management" processes are provided here.

11.4.1. State Portal – Primary Life Cycle Phases and Deliverables

Stage	Phase	Reference	Deliverables / Artifacts	Description
Acquisition	RFP Preparation	[1]	Business Requirements	Business requirements should provide information such as objectives of State Portal, expected benefits, classes of users, high level functionalities etc.
		[2]	Detailed Project Report (DPR)	Detailed project report should contain • Gap analysis of departmental applications with respect to State Portal reference framework • Technical feasibility • High level project plan • Budgetary cost estimates
		[3]	RFP Document	Request for Proposal document contains all the information required by vendors for submitting their technical solution and commercial quotations.
	Vendor Selection	[4]	Bid Evaluation Report	Invited Vendors will provide the responses for implementation of State Portal in the designated format. Following are few high level views that vendor responses should contain: • Vendors Market share • Vendors financial information • Vendors prior experience in similar projects • Technical solution

Stage	Phase	Reference	Deliverables / Artifacts	Description
				• Cost and Timelines • Assumptions • Sample profiles that would be part of the project • References, if any Bid evaluation committee would prepare a bid evaluation report taking into consideration technical solution, commercials, quality of vendor and other defined criteria.
	Contract Agreement	[5]	Contract Agreement Document	The contract agreement document should contain but not limited to: • Definitions and interpretations of terms and terminologies • Conditions precedent • Objectives and scope of contract • Commencement and duration of agreement • Scope and provision of services • Approvals and required consents • Use and acquisition of assets • Access to concerned state agency locations • Security and safety • Cooperation • Financial issues (Terms of payment, Invoicing and settlement) • Contract Termination (Termination of agreement and Effects of termination) • Protection and Limitations • Warranties • Third party claims • Limitations of liabilities • Force majeure • Data protection • Confidentiality • Audit access and reporting • Intellectual properties • Serviceability and waivers • Survivability • Compliance with laws and regulations • Ethics • Disputes and Law (Dispute resolution, Applicable law and jurisdiction) • Change control • Change management • Exit management • Transfer of assets • Confidential information, security and data

Stage	Phase	Reference	Deliverables / Artifacts	Description
				• Escalation • Invoicing and settlement • Project timelines
	Contract Monitoring	[6]	Monitoring Reports	Contract monitoring report should contain: • Progress of the project • Status of various activities and deliverable • Issues and concerns (if any) • Action items with responsibility and time frame • Status of action items from previous cycle
Design and development	Requirements Analysis	[7]	Requirements Specifications	The system requirements specification should include: a) Generic specification information; b) System identification and overview; c) Required states and modes; d) Requirements for the functions and performance of the system; e) Business, organizational, and user requirements; f) Safety, security, and privacy protection requirements; g) Human-factors engineering (ergonomics) requirements; h) Operations and maintenance requirements; i) System external interface requirements; j) System environmental requirements; k) Design constraints and qualification requirements; l) Computer resource requirements: 1) Computer hardware requirements; 2) Computer hardware resource requirements, including utilization requirements; 3) Computer software requirements; 4) Computer communications requirements. m) System quality characteristics; n) Internal data requirements; o) Installation-dependent data requirements; p) Physical requirements; q) Personnel, training, and logistics requirements; r) Packaging requirements; s) Precedence and criticality of requirements; t) Rationale. The software requirements specification should include a) Generic description information

Stage	Phase	Reference	Deliverables / Artifacts	Description
				b) System identification and overview; c) Functionality of the software item, including 1) Performance requirements; 2) Physical characteristics; 3) Environmental conditions. d) Requirements for interfaces external to software item; e) Qualification requirements; f) Safety specifications, including those related to methods of operation and maintenance, environmental influences, and personnel injury; g) Security and privacy specifications, including those related to compromise of sensitive information; h) Human-factors engineering (ergonomics) requirements, including those for 1) Manual operations; 2) Human-equipment interactions; 3) Constraints on personnel; 4) Areas that need concentrated human attention and are sensitive to human errors and training. i) Data definition and database requirements, including installation-dependent data for adaptation needs; j) Installation and acceptance requirements of the delivered software product at the operation site(s); k) Installation and acceptance requirements of the delivered software product at the maintenance site(s); l) User documentation requirements; m) User operation and execution requirements; n) User maintenance requirements; o) Software quality characteristics; p) Design and implementation constraints; q) Computer resource requirements; r) Packaging requirements; s) Precedence and criticality of requirements; t) Requirements traceability; u) Rationale.
		[8]	Traceability Document	• Identify each requirement with unique ID • Traceability between RFP and requirements Specifications
	Architecture Design	[9]	Architecture Design Document	The system architecture description should include a) Generic description information; b) System overview and identification;

Stage	Phase	Reference	Deliverables / Artifacts	Description
				c) Hardware item identification; d) Software item identification; e) Manual operations identification; f) Concept of execution; g) Rationale for allocation of hardware items, software items, and manual operations. The software architecture should include: a) Generic description information b) System overview and identification c) Software item architectural design, including 1) Software architecture general description; 2) Software component definition; 3) Identification of software requirements allocated to each software component; 4) Software component concept of execution; 5) Resource limitations and the strategy for managing each resource and its limitation. d) Rationale for software architecture and component definition decisions, including database and user interface design. Other information should include: • Architectural Goals and Constraints • Layered View • Logical View • Use Case View • Deployment view • Package Hierarchy • Realization of architectural requirements • Content taxonomy • Metadata specifications • Master data specifications
		[10]	Traceability Document	Traceability between requirements specifications and architecture design
	Detailed Design	[11]	Detailed Design Document	The software item design description should include a) Generic description information b) Description of how the software item satisfies the software requirements, including algorithms and data structures; c) Software item input/output description; d) Static relationships of software units; e) Concept of execution, including data flow and control flow; f) Requirements traceability:

Stage	Phase	Reference	Deliverables / Artifacts	Description
				1) Software component-level requirements traceability; 2) Software unit-level requirements traceability. g) Rationale for software item design; h) Reuse element identification. Other information should include: • Defines the user's interaction with the State Portal. • Wire frames (user interface layout) • Prototype (with clickable user interface)
		[12]	Traceability Document	Traceability between requirements specifications, architecture design and detailed design
	Coding	[13]	Source Code	• Identification of the software, including the name and date of revision and/or version, as applicable. • Source code listing
		[14]	Traceability Document	Traceability between requirements and code
	Testing	[15]	Test Plan	The test plan should contain a) Generic plan information b) Test levels; c) Test classes; d) General test conditions; e) Test progression; f) Data recording, reduction, and analysis; g) Test coverage (breadth and depth) or other methods for assuring sufficiency of testing; h) Planned tests, including items and their identifiers; i) Test schedules; j) Requirements traceability; k) Qualification testing environment, site, personnel, and participating organizations.
		[16]	Test Cases	A test case specification shall have the following structure: a) Test case specification identifier; b) Test items; c) Input specification; d) Output specifications; e) Environmental needs; f) Special procedural requirements; g) Inter case dependencies.
		[17]	Traceability	Traceability between requirements specifications, architecture design, detailed design and

Stage	Phase	Reference	Deliverables / Artifacts	Description
			Document	test cases
		[18]	Test Reports	The test report should include a) Generic report information b) System identification and overview; c) Overview of test results, including 1) Overall assessment of the software tested; 2) Impact of test environment. d) Detailed test results, including 1) Test identifier; 2) Test summary; 3) Problems encountered; 4) Deviations from test cases/ procedures. e) Test log; f) Rationale for decisions.
Acceptance	Acceptance Testing	[19]	Test Plan	A test plan should have the following structure: a) Test plan identifier; b) Introduction; c) Test items; d) Features to be tested; e) Features not to be tested; f) Approach; g) Item pass/fail criteria; h) Suspension criteria and resumption requirements; i) Test deliverables; j) Testing tasks; k) Environmental needs; l) Responsibilities; m) Staffing and training needs; n) Schedule; o) Risks and contingencies; p) Approvals.
		[20]	Test Reports	The test report should include a) Generic report information b) System identification and overview; c) Overview of test results, including 1) Overall assessment of the software tested; 2) Impact of test environment. d) Detailed test results, including

Stage	Phase	Reference	Deliverables / Artifacts	Description
				1) Test identifier; 2) Test summary; 3) Problems encountered; 4) Deviations from test cases/ procedures. e) Test log; f) Rationale for decisions.
	Release/ Deployment	[21]	Deployment Plan	Deployment plan should include • Deployment Scope • Deployment Architecture • Deployment Strategy (roll out strategy) • Deployment Schedule • Deployment Costs • Deployment Communication plan
Operation and Maintenance	User Training	[22]	Training Plan and Records	Two major types of audience are addressed in these training requirements: • Individuals who will use the State Portal for content and service related operations. • Individuals who will install and provide operations support for the product Training Plan document describes the basic training resource and timing requirements, and a high level description of the performance objectives to be achieved through training of the users and the operations support staff for the product under development
	Operation	[23]	Operation Plan	The operation plan should include a) Generic plan information for the following activities: 1) Operation process implementation; 2) Operational testing; 3) System operation; 4) User support. b) Specific standards, methods, tools, actions, procedures, and responsibility associated with the operation of software. Operation plan should also address • Application/ Infrastructure Monitoring and Management Policy • Security policy • Data security policy • Content management policy • Data Backup policy • List of administration tools to be used for system, OS, and COTS products, which includes Database server, application server etc. These tools are provided as part of respective products.

Stage	Phase	Reference	Deliverables / Artifacts	Description
				• Disaster Recovery Plan
	User Support	[24]	Records	Problem Reports, Tickets, Resolution Records
	Performance Monitoring	[25]	Performance Reports	• List of tools for application/ infrastructure monitoring and management of State Portal • Monitoring reports to be published and their periodicity (For ex: Application Uptime, Response Time, Server Uptime etc) A report should be prepared quarterly. It should contain following type of information: • Data about quality attributes such as response times, system uptime, application uptime, security, internet connectivity, incidents, unplanned downtimes etc. • Usage analysis report • Application log analysis report • Status of action items from previous cycle • Issues and concerns (if any)
	Maintenance	[26]	Maintenance Plan	The maintenance plan should include a) Generic plan information for the following activities: 1) Maintenance process implementation; 2) Problem and modification analysis; 3) Modification implementation; 4) Maintenance review/acceptance; 5) Migration; 6) Software retirement. b) Specific standards, methods, tools, actions, procedures, and responsibility associated with the maintenance process.
		[27]	Maintenance Records	Problem Reports, Change Requests, Change Records

11.4.2. State Portal – Supporting Life Cycle Processes and Deliverables

Process	Reference	Deliverables / Artifacts	Description
Project Management	[28]	Project Plan	The project management plan should include: a) Generic plan information for managing the project; b) Project organizational structure showing authority and responsibility of each organizational unit, including external organizations; c) Engineering environment (for development, operation or maintenance, as applicable), including test environment, library, equipment, facilities, standards, procedures, and tools;

Process	Reference	Deliverables / Artifacts	Description
			d) Work breakdown structure of the life cycle processes and activities, including the software products, software services and non-deliverable items to be performed, budgets, staffing, physical resources, software size, and schedules associated with the tasks; e) Management of the quality characteristics of the software products or services (Separate plans for quality may be developed.); f) Management of safety, security, privacy, and other critical requirements of the software products or services (Separate plans for safety and security may be developed.); g) Subcontractor management, including subcontractor selection and involvement between the subcontractor and the acquirer, if any; h) Quality assurance; i) Verification and validation, including the approach for interfacing with the verification and validation agent, if specified; j) Acquirer involvement (i.e., joint reviews, audits, informal meetings, reporting, modification and change, implementation, approval, acceptance, access to facilities); k) User involvement (i.e., requirements setting exercises, prototype demonstrations and evaluations); l) Risk management (i.e., the management of the areas of the project that involve technical, cost, and schedule risks); m) Security policy (i.e., the rules for need-to-know and access-to-information at each project organizational level); n) Approval required by such means as regulations, required certifications, proprietary, usage, ownership, warranty and licensing rights; o) Means for scheduling, tracking, and reporting; p) Training of personnel; q) Software life cycle model; r) Configuration management. Integrated Project plan should include: • List of project activities and milestones • Dependencies • Availability of Departmental Applications • Resource Loading
	[29]	Project Monitoring Records	Project monitoring reports for Progress tracking against plans and specifications, including • product size • project effort, cost, and schedule • activities • risks Control actions when discrepancies between plans and actual progress occur.
Configuration	[30]	Configuration Management	The software configuration management plan should include a) Generic plan information for the following activities:

Process	Reference	Deliverables / Artifacts	Description
Management		Plan	1) Configuration management process implementation; 2) Configuration identification; 3) Configuration control; 4) Configuration status accounting; 5) Configuration evaluation; 6) Release management and delivery. b) Relationship with organizations such as software development or maintenance.
	[31]	Configuration Management Records	The software configuration management records should include a) Generic record information for the following activities: 1 Configuration management process implementation; 2) Configuration identification; 3) Configuration control; 4) Configuration status accounting; 5) Configuration evaluation; 6) Release management and delivery.
Quality Assurance	[32]	Quality Assurance Plan	The software quality assurance plan should include a) Generic plan information for software quality assurance; b) Quality standards, methodologies, procedures, and tools for performing the quality assurance activities (or their references in organization's official documentation); c) Procedures for contract review and coordination thereof; d) Procedures for identification, collection, filing, maintenance, and disposition of quality records; e) Resources, schedule(s), and responsibilities for conducting the quality assurance activities; f) Selected activities and tasks from supporting processes such as Verification, Validation, Joint Review, Audit, and Problem Resolution.
	[33]	Quality Assurance Records	Provide evidence of the accomplishment of quality assurance activities. Records should include reports of review, audit & tests conducted on various artefacts/ work products at different phases of life cycle as per QA plan.
Content Management	[34]	Content Management Plan	Content Management Plan should address as per defined workflows & responsibilities assigned: • Content Management Policy • Content scope • Content Management Workflow • Content preparation • Content review • Content publishing • Content updation • Content archival
	[35]	Content currency report	This report should be prepared periodically (suggested once per quarter). It should contain information such as:

Process	Reference	Deliverables / Artifacts	Description
			• Summary of content change requests • Number of documents published, modified, exited • Usage analysis of various types of content Important events covered and missed

11.4.3. State Portal – Information Security Management Processes and Deliverables

Process	Reference	Deliverables/ Artifacts	Description
Information Security Management Processes	[36]	Security Policy Document	
	[37]	Asset Management Plan & Procedure	
	[38]	Risk Management Plan & Procedure	
	[39]	Human Resources Security Plan & Procedure	
	[40]	Physical & Environmental Security Plan & Procedure	
	[41]	Communications & Operations Management Plan & Procedure	
	[42]	Access Control Plan & Procedure	
	[43]	Information Systems Acquisition, Development & Maintenance Plan & Procedure	
	[44]	Information Security Incident Management Plan & Procedure	
	[45]	Business Continuity Management Plan & Procedure	

11.4.4. State Portal – IT Service Management Processes and Deliverables

Process	Reference	Deliverables/ Artifacts	Description
IT Service Management Processes	[46]	Policy Document	
	[47]	Plan & Procedure for Service Delivery Processes: • Service Level Management • Service Reporting	

Process	Reference	Deliverables/ Artifacts	Description
		• Service Continuity & Availability Management • Budgeting & Accounting for IT Services • Capacity Management • Information Security Management	
	[48]	Plan & Procedure for Relationship Processes: • Business Relationship Management • Supplier Management	
	[49]	Plan & Procedure for Resolution Processes: • Incident Management • Problem Management	
	[50]	Plan & Procedure for Control Processes: • Configuration Management • Change Management	
	[51]	Plan & Procedure for Release Process: • Release Management Process	

11.5. How to Use Compliance Checklist

This compliance checklist should be used for performing compliance verification of all work products or artefacts produced during state portal implementation process and there after. Checklist provides list of “Compliance Items”, to be verified. For each compliance item, applicable guidelines are provided in the “Guideline Reference” section number of State Portal Framework document. “Artefacts to be verified” column mentions the list of artifacts to be referred for compliance verification. After checking compliance, section number of verified artifact should be mentioned in “Artefact Reference” column.

11.6. Compliance Checklist

11.6.1. State Portal Requirements

11.6.1.1. Information Categories

No	Compliance Item	Guideline Reference	Artefacts to be Verified	Artefact Reference	Yes/No/ NA	Remarks
1.	About State government, Departments, Organisations	2.1	[7], [8], [9], [10], [15], [16], [17]			

2.	Sector/ Regional profile	2.1	[7], [8], [9], [10], [15], [16], [17]			
3.	Programmes and Schemes	2.1	[7], [8], [9], [10], [15], [16], [17]			
4.	Services	2.1	[7], [8], [9], [10], [15], [16], [17]			
5.	Application forms	2.1	[7], [8], [9], [10], [15], [16], [17]			
6.	Acts and rules	2.1	[7], [8], [9], [10], [15], [16], [17]			
7.	Documents and Reports	2.1	[7], [8], [9], [10], [15], [16], [17]			
8.	Circulars and Notifications	2.1	[7], [8], [9], [10], [15], [16], [17]			
9.	Tenders	2.1	[7], [8], [9], [10], [15], [16], [17]			[Optional]
10.	Recruitments	2.1	[7], [8], [9], [10], [15], [16], [17]			[Optional]
11.	News and press release	2.1	[7], [8], [9], [10], [15], [16], [17]			
12.	Contact details	2.1	[7], [8], [9], [10], [15], [16], [17]			
13.	Events/Announcements	2.1	[7], [8], [9], [10], [15], [16], [17]			[Optional]
14.	Discussion forums and chat rooms	2.1	[7], [8], [9], [10], [15], [16], [17]			[Optional]

11.6.1.2. Transactional Government Services

Note: This is only suggested list of services. State would define required list of service.

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
1.	Registration and Issuance of Birth Certificate	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
2.	Registration and Issuance of Death Certificate	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
3.	Immovable Property tax collection	2.2	[7], [8], [9], [10], [15], [16],			[Optional]

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
			[17]			
4.	New Water Tap Connection	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
5.	Collection of Energy Charges	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
6.	New Electricity Connection	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
7.	Enhancement of existing connection into higher load connection	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
8.	Dues list / Duplicate bill generation	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
9.	Complaints Registration	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
10.	Issue of Non- Encumbrance Certificate	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]
11.	Issue of Certified Copy of documents	2.2	[7], [8], [9], [10], [15], [16], [17]			[Optional]

11.6.2. Portal Functionalities

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
1	Metadata replication	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
2	Content management	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
3	Full text Search	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
4	Metadata based search	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
5	Information browser	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			Optional

6	Personalization	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			Optional
7	Portal usage reports	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
8	Self service	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			Optional
9	Notifications	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			Optional
10	FAQ	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
11	Portal administration	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
12	CSC locator	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
13	Government office locator	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			
14	Send a email to government	2.3	[7], [8], [9], [10], [11], [16], [17], [18]			

11.6.3. Architectural Requirements

No	Compliance Item	Guideline Reference	Artifact to be Verified	Artifact Reference	Yes/No/ NA	Remarks
1.	Performance	2.4.1	[7], [9], [16], [17], [18]			
2.	Scalability	2.4.2	[7], [9], [16], [17], [18]			
3.	High availability	2.4.3	[7], [9], [16], [17], [18]			
4.	Portability	2.4.4	[7], [9], [16], [17], [18]			
5.	Extensibility	2.4.5	[7], [9], [16], [17], [18]			
6.	Multi lingual user interface	2.4.6	[7], [9], [16], [17], [18]			
7.	Interoperability	2.4.7	[7], [9], [16], [17], [18]			
8.	Universal accessibility	2.4.8	[7], [9], [16], [17], [18]			
9.	Security	2.4.9	[7], [9], [16], [17], [18]			
10.	Access points and access devices	2.4.10	[7], [9], [16], [17], [18]			

11.6.4. State Portal Architecture

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/NA	Remarks
	Usage of Off the shelf software products and tools					
1	Identified off the shelf software products and tools provide specified functionality? (Complete below list during compliance verification.)	3	[9], [10], [11]			
	Operating system	3	[9], [10], [11]			
	Database management system	3	[9], [10], [11]			
	Web content management system	3	[9], [10], [11]			
	Web server	3	[9], [10], [11]			
	Application server	3	[9], [10], [11]			
	Service registry	3	[9], [10], [11]			
	Service repository	3	[9], [10], [11]			
	Directory server	3	[9], [10], [11]			
	Secure proxy server	3	[9], [10], [11]			
	Web log analyzer	3	[9], [10], [11]			
	Management and monitoring tools	3	[9], [10], [11]			
	Other products/tools	3	[9], [10], [11]			
2	Identified off the shelf software products and tools supports defined architectural requirements? (Complete below list during compliance verification.)	3	[9], [10], [11], [16], [17], [18]			
	Operating system	3	[9], [10], [11], [16], [17], [18]			
	Database management system	3	[9], [10], [11], [16], [17], [18]			
	Web content management system	3	[9], [10], [11], [16], [17], [18]			
	Web server	3	[9], [10], [11], [16], [17], [18]			
	Application server	3	[9], [10], [11], [16], [17], [18]			
	Service registry	3	[9], [10], [11], [16], [17], [18]			
	Service repository	3	[9], [10], [11], [16], [17], [18]			
	Directory server	3	[9], [10], [11], [16], [17], [18]			
	Secure proxy server	3	[9], [10], [11], [16], [17], [18]			
	Web log analyzer	3	[9], [10], [11], [16], [17], [18]			

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/NA	Remarks
	Management and monitoring tools	3	[9], [10], [11], [16], [17], [18]			
	Other products/tools	3	[9], [10], [11], [16], [17], [18]			
	Architectural Guidelines					
3	Does architecture follow layered architecture pattern and classifies architectural components into specified layers?	3.2	[9], [10]			
4	All architectural components provide only the "class of functionality" expected from the layer they belong to?	3.2	[9], [10]			
5	Does architecture support defined access devices, access points and browsers?	3.2.1	[9], [10], [16], [17], [18]			
6	Is realization of following service modules conforms to specified guidelines? a. Transactional government service b. Web-form service c. MDR service d. Other services	3.3.3.1	[9], [10], [16], [17], [18]			
7	Is realization of following functional modules explained adequately? a. User management b. Self service c. Reporting d. Search e. Notifications f. Content management g. Content feeds	3.3.3.2	[9], [10], [16], [17], [18]			
8	Is realization of following content management modules explained adequately? a. Content delivery b. Content authoring c. Content workflow d. Content feeds	3.3.3.3	[9], [10], [16], [17], [18]			
9	Are specific components provided for defined set of utility features?	3.3.3.4	[9], [10], [16], [17], [18]			

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
10	Is "common service communication infrastructure" component in use, provides defined functionality?	3.3.4.1	[9], [10]			Optional
11	Are adapters available for proposed off the shelf software applications?	3.2.4.2	[9], [10]			Optional
12	Is relational database management system used for managing structured data?	3.3.5.1	[9], [10], [11], [12]			
13	Is unstructured data not stored in content repository, which is based on database server?	3.3.5.2, 3.3.5.3	[9], [10], [11], [12]			Optional
14	Is user profile related information managed using directory server?	3.3.5.4,	[9], [10], [11], [12]			Optional
15	Is access control related information managed using "access control system"?	3.3.5.6	[9], [10], [11], [12]			Optional
16	Are transactional government services published to state service registry and repository?	3.3.6.1	[9], [10], [16], [17], [18]			
17	Are transactional government services published to national service repository and repository?	3.3.6.1	[9], [10], [16], [17], [18]			
	Monitoring and management					
18	Is there a defined policy for monitoring and management?	3.3.7	[23]			
19	Are suitable tools used for infrastructure monitoring and administration?	3.3.7	[9], [23],[25]			Optional
20	Are suitable tools used for application monitoring and administration?	3.3.7	[9], [23],[25]			Optional
21	Are defined management and monitoring related reports produced periodically?	3.3.7	[9], [23],[25]			Optional
22	Is there a defined policy for data backup and restore?	3.3.7	[23],[41]			
23	Is data backup performed as per defined policy?	3.3.7	[23],[41]			
	Realizing Architectural requirements					
24	Does architecture adhere to defined	3.6.1	[9], [10], [16], [17], [18]			

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/NA	Remarks
	guidelines to provide performance?					
25	Does architecture adhere to defined guidelines to provide scalability?	3.6.2	[9], [10], [16], [17], [18]			
26	Does architecture adhere to defined guidelines to provide high availability at network level?	3.6.3	[9], [10], [16], [17], [18]			
27	Does architecture adhere to defined guidelines to provide high availability at hardware level?	3.6.3	[9], [10], [16], [17], [18]			
28	Does architecture adhere to defined guidelines to provide high availability at COTS software level?	3.6.3	[9], [10], [16], [17], [18]			
29	Does architecture adhere to defined guidelines to provide high availability at application level?	3.6.3	[9], [10], [16], [17], [18]			
30	Does architecture adhere to defined guidelines to provide portability?	3.6.4	[9], [10], [16], [17], [18]			
31	Does architecture adhere to defined guidelines to provide extensibility?	3.6.5.	[9], [10], [16], [17], [18]			
32	Does architecture adhere to defined guidelines to provide multi lingual interface?	3.6.6	[9], [10], [16], [17], [18]			
33	Does architecture adhere to defined guidelines to provide interoperability?	3.6.7	[9], [10], [16], [17], [18]			
34	Does architecture adhere to defined guidelines to provide universal accessibility?	3.6.8	[9], [10], [16], [17], [18]			
	Security					
35	Are defined guidelines followed for maintaining confidentiality of user's data?	3.6.9	[9], [10], [16], [17], [18], [36], [41], [42]			
36	Is architecture complies with defined guidelines for authentication?	3.6.9.1	[9], [10], [16], [17], [18], [36], [41], [42]			
37	Is architecture complies with defined guidelines for authorization?	3.6.9.2	[9], [10], [16], [17], [18], [36], [41], [42]			
38	Is access to transactional government services controlled as per defined policy?	3.6.9.4	[9], [10], [16], [17], [18], [36], [41], [42]			
39	Is defined part of portal functionality available only over HTTPS protocol?	3.6.9.5	[7], [16], [17], [18]			

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/NA	Remarks
40	Is public functionality accessible without signing-in?	3.6.9.6	[9], [10], [16], [17], [18], [36], [41], [42]			
41	Is URL based security is adopted for implementing authentication and authorization?	3.6.9.6	[9], [10], [16], [17], [18], [36], [41], [42]			Optional
42	Is single sign-on implemented for all transactional government services, portal services?	3.6.9.7	[9], [10], [16], [17], [18], [36], [41], [42]			
43	Are defined guidelines followed to provide data security?	3.6.9.10	[9], [10], [16], [17], [18], [36], [41], [42]			

11.6.5. Content Management

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/NA	Remarks
1.	Does State Portal content adhere to defined content format standards?	5.3	[7], [16], [17], [18], [34], [35]			
2.	Is content contracts adhere to defined standards?	5.4.1	[7], [16], [17], [18], [34], [35]			Optional
3.	Does content management system provide defined functionality?	5.5	[7], [16], [17], [18], [34], [35]			
4.	Is CMS supports defined content management policies?	5.5	[7], [16], [17], [18], [34], [35]			
5.	Is content management system provides content authoring tools with defined functionality?	5.5, 5.5.1	[7], [16], [17], [18], [34], [35]			
6.	Does content management system (CMS) support meta data capture during content authoring and publishing?	5.5.1	[7], [16], [17], [18], [34], [35]			

11.6.6. Content Integration

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
1.	Is content sourcing scenario “Sourced in paper form” supported?	6.2.1	[7], [16], [17], [18], [34], [35]			
2.	Is content sourcing scenario “Sourced from other government web sites” supported?	6.2.2	[7], [16], [17], [18], [34], [35]			
3.	Is content sourcing from private or third parties supported?	6.2.3	[7], [16], [17], [18], [34], [35]			
4.	Are content feeds supported?	6.2.4	[7], [16], [17], [18], [34], [35]			Optional
5.	Is links to external sourced supported	6.2.5	[7], [16], [17], [18], [34], [35]			
6.	Is content discovery within State Portal supported?	6.4.1	[7], [16], [17], [18], [34], [35]			
7.	Does content taxonomy conform to defined standard?	6.5.1	[7], [16], [17], [18], [34], [35]			
8.	Does State Portal implement standardized metadata schema?	6.5.2	[7], [16], [17], [18], [34], [35]			
9.	Does State Portal implement standardized master data schema for metadata?	6.5.3	[7], [16], [17], [18], [34], [35]			
10.	Does Content publishing workflow enforce taxonomy rules?	6.5.4	[7], [16], [17], [18], [34], [35]			
11.	Does Content publishing workflow enforce definition of metadata attributes	6.5.4	[7], [16], [17], [18], [34], [35]			
12.	Does Content publishing workflow makes it mandatory to define metadata?	6.5.4	[7], [16], [17], [18], [34], [35]			
13.	Does content publishing workflow conform to defined guidelines?	6.5.4	[7], [16], [17], [18], [34], [35]			
14.	Are content objects uniquely identifiable using a unique ID?	6.5.6	[7], [16], [17], [18], [34], [35]			
15.	Is metadata of published content propagated to consolidated metadata repository as per defined process?	6.5.7	[7], [16], [17], [18], [34], [35]			
16.	Is propagated metadata normalized before saving into consolidated metadata repository?	6.5.8	[7], [16], [17], [18], [34], [35]			
17.	Is change management process defined to manage metadata schema changes?	6.5.9	[30], [50]			
18.	Is change management process defined for managing master data changes?	6.5.10	[30], [50]			

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
19.	Is updated metadata of published content propagated to consolidated metadata repository periodically?	6.5.11	[7], [16], [17], [18], [34], [35]			
20.	Is web based interface of content repository provides defined functionality?	6.5.12	[7], [16], [17], [18], [34], [35]			
21.	Is explorer type of user interface provided for browsing information provided on State Portal?	6.6.2.2	[7], [16], [17], [18], [34], [35]			
22.	Is search functionality accessible as a service?	6.6.2.4	[7], [16], [17], [18], [34], [35]			
23.	Does user interface of search functionality provide defined functionality?	6.6.2.3	[7], [16], [17], [18], [34], [35]			
24.	Is there a well identified component responsible of replicating metadata changes from State Portal's content repository to consolidated metadata repository?	6.7	[9]			
25.	Does MDR service provide defined functionality?	6.7	[7], [16], [17], [18], [34], [35]			
26.	Does MDR service interoperate with metadata consolidation server?	6.7, 6.8	[7], [16], [17], [18], [34], [35]			
27.	Is MDR service deployable on web-service based "service communication infrastructure"?	6.7	[7], [16], [17], [18], [34], [35]			

11.6.7. Integration and Management of Transactional Government Services

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
1.	Are transactional government services deployable on web-service based "service communication infrastructure"?	7.1	[9], [10], [11], [12]			
2.	Are transactional government services deployable on SSDG based "service communication infrastructure"?	7.1.2	[9], [10], [11], [12]			
3.	Does transactional government services adheres to defined standards?	7.2.8	[9], [10], [11], [12]			
4.	Is right form of integration approach is	7.3	[9], [10], [11], [12]			

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
	used for implementing every transactional government service?					
5.	Is Web form implemented as per defined standards?	7.4	[9], [10], [11], [12], [16], [17], [18]			
6.	Is Data level integration implemented as per defined standards?	7.5	[9], [10], [11], [12], [16], [17], [18]			
7.	Is application level integration implemented as per defined standards?	7.6	[9], [10], [11], [12], [16], [17], [18]			
8.	Is service level integration implemented as per defined standards?	7.8	[9], [10], [11], [12], [16], [17], [18]			

11.6.8. Indian government Guidelines

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
1.	Does state portal implementation complies with checklist items mentioned in “Compliance Matrix” section of “Guidelines for Indian Government Websites” document?	8	[16], [17], [18]			

11.6.9. Overall State Portal Functionality

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No/ NA	Remarks
1.	Does State Portal provide information of defined categories?	2.1	[7], [8], [9], [10], [11], [12], [16], [17], [18]			
2.	Does State Portal provide defined transactional government services?	2.2	[7], [8], [9], [10], [11], [12], [16], [17], [18]			

3.	Does State Portal provide defined portal functionality?	2.3	[7], [8], [9], [10], [11], [12], [16], [17], [18]			
4.	Do State Portal meets defined standards architectural requirements?	2.4	[7], [8], [9], [10], [11], [12], [16], [17], [18]			
5.	Do State Portal provides defined architectural components?	3	[7], [8], [9], [10], [11], [12], [16], [17], [18]			
6.	Does State Portal provide defined content management framework?	5	[7], [8], [9], [10], [11], [12], [16], [17], [18]			
7.	Does State Portal provide defined content integration functionality?	6	[7], [8], [9], [10], [11], [12], [16], [17], [18]			
8.	Does State Portal conform to defined integration approach for transactional government services?	7	[7], [8], [9], [10], [11], [12], [16], [17], [18]			
9.	Does the user interface conform to defined user interface design guidelines?	8	[7], [8], [9], [10], [11], [12], [16], [17], [18]			

11.6.10. State Portal Status and Progress Monitoring

No	Compliance Item	Guideline Reference	Artifacts to be Verified	Artifact Reference	Yes/No / NA	Remarks
1.	Is performance / response time (worst, average, best) within defined limits?	NA	[25]			
1.	Is application uptime within defined limits?	NA	[25]			
2.	Is content published within planned timelines?	NA	[25]			
3.	Is availability of transactional government services within defined limits?	NA	[25]			
4.	Is change requests got closed within planned timelines?	NA	[25]			
5.	Is internet bandwidth utilization within defined limits?	NA	[25]			
6.	Is data backed up as per defined policies?	NA	[25]			
7.	Is security audit performed as per defined policy?	NA	[25]			
8.	There were no instances of broken links such as “page not found”?	NA	[25]			
9.	There were no application related errors such as “system exception”?	NA	[25]			

10.	There were no application related errors in transactional government services?	NA	[25]			
11.	There were no security violations?	NA	[25]			
12.	There were no instances of unplanned application downtime?	NA	[25]			
13.	There were no instances of unplanned application restarts?	NA	[25]			
14.	There were no network outages?	NA	[25]			