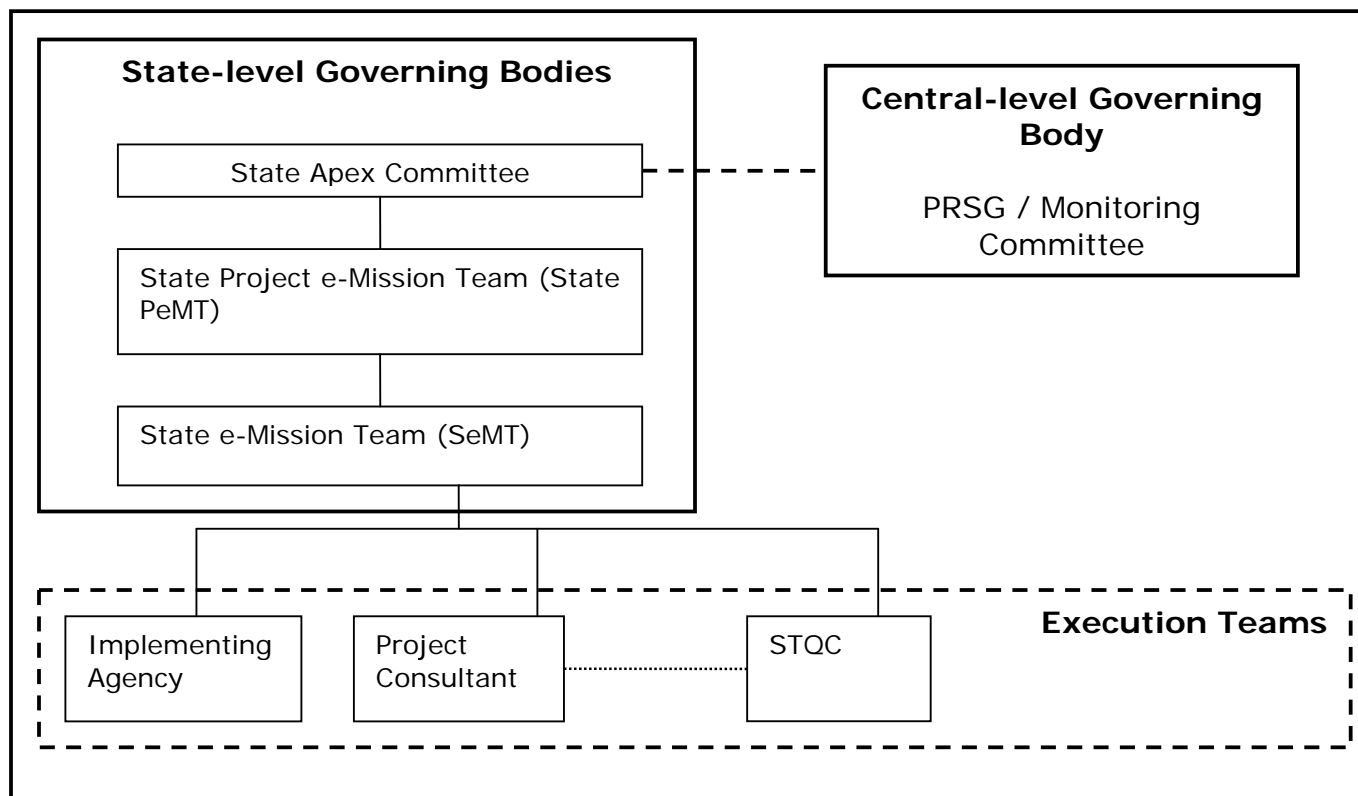# 10. Governance Framework

The Governance Framework for State Portal Framework are divided in Central Level and State Level. Following is the brief description of the same. For details, please refer to the Operational Guidelines available on DIT Website.

Following figure gives the overall Governance Structure:

A. Central Level Governance

A PRSG or the monitoring committee shall review the financial and technical progress of the project and advice the project executing team on new directions/approach. It will also link-up with the work going on elsewhere in the country for full utilization of the capabilities available in the country. It shall also review the deliverables of the agencies involved and amends the deliverables if required keeping in view the project objective. The suggested composition of this committee is given in the following table.

- Secretary, DIT
- Additional Secretary (eGovernance), GoI
- Secretary IT (Respective State/ UT)
- Director(CSC), GoI
- NIC Representative
- CDAC Representative
- DFA, DIT
- Director (eGov)/ Joint Director (eGov), GoI
- Joint Secretary (eGovernance), GoI

B. State Level Governance

At the State level, the State Project e-Mission Team (State PeMT) shall use the State e-Mission Team (SeMT) to oversee the implementation of the project at state level.

SeMT shall interact with all the internal departments and also the CSP, selected implementing agency, project consultant and STQC for successful implementation of the project. SeMT shall also interact, on need basis, with CDAC and NIC on issues regarding SSDG and State Portal Framework respectively.

The suggested composition of each of the governing bodies described in the earlier figure is as follows:
1. State Apex Committee
- Chief Secretary
- State IT Secretary
- Representative of Fin. Dept.
- NIC Representative
- Principal Secretaries/Secretaries of concerned Departments
- Any other person deemed fit by Chief Secretary

2. State Project e-Mission Team (State PeMT)
- IT Secretary (Mission Leader)

- Dedicated full-time HOD/Director
- HODs/Representatives from concerned departments
- NIC Representative
- Nominated CDAC Representative

- Internal domain specialist(full-time) (from SeMT)
- Internal technical full-time representatives (from SeMT)
- Any other person deemed fit by Mission Leader

3. SeMT is setup under the nodal agency in the State.

For more details of the above governance structures, please refer to stage 4 and Stage 5 described in the Operational Guidelines available on the DIT website at following URL:
http://www.mit.gov.in/download/GuideforOperationalModel4.0.pdf/

10.1. Need for Governance Framework

Some of the functions of the 'Governance Organization' would be strategic in nature to increase the usability of the state portal, strategies, communication and awareness policy and some would be day to day routine operations to ensure smooth functioning of the portal. Following are some of the key tasks to be performed by the Governance Organization for State Portal project:

a) Compliance to the framework provided by Department of IT, Govt. of India

b) Make State Portal usable for delivery of various services

c) Coordinate / liaison with user agencies/ departments (to offer/integrate more services in State Portal service basket)

d) Deal with policy matters such as standardization, usage policy, dispute resolution etc.

e) Manage operational issues on an ongoing basis

f) Policy for management and updating information/content related to services to be offered through State Portal

g) Managing and monitoring of IT Infrastructure and other related IT support functions required for State Portal

The above tasks have been envisaged based on understanding of critical needs of the State Government with respect to the State Portal. The role of the 'Governance Organization', and its responsibilities at various tiers, has been proposed on the basis of the study of existing governance organizations for various IT projects. Most of the states across the country already have top level committees for implementation of large scale IT projects. These committees have been formed either under the chairmanship of Chief Minister or Chief Secretary and Steering Committees under respective departmental secretaries. In case a committee/governance setup already exists in

the state, it is proposed to leverage this existing setup for state portal implementation and its operationalisation otherwise a new governance setup would need to be formed.

10.2. Governance Processes

There would be many processes involved for various roles in the governance organization. Although the states would be given a standardized templates and structure of documents by the DIT, Government of India for but these document(s) would need to be customized as per the state needs.

10.3. Artefacts or Deliverables

10.3.1 State Portal – Primary Life Cycle Phases and Deliverables

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
Acquisition	RFP Preparation	Business Requirements	Business requirements should provide information such as objectives of State Portal, expected benefits, classes of users, high level functionalities etc.	ISO 12207
		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	ISO 12207
		RFP Document	Request for Proposal document contains all the information required by vendors for submitting their technical solution and commercial quotations.	ISO 12207
	Vendor Selection	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 • Cost and Timelines	ISO 12207

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
			• 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	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	ISO 12207

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
			• Disputes and Law (Dispute resolution, Applicable law and jurisdiction) • Change control • Change management • Exit management • Transfer of assets • Confidential information, security and data • Escalation • Invoicing and settlement • Project timelines	
	Contract Monitoring	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	ISO 12207

Design and development	Requirements Analysis	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;
				ISO 12207/ IEEE 830

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines

			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
			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	

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
			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.	
		Traceability Document	• Identify each requirement with unique ID • Traceability between RFP and requirements Specifications	ISO 12207/ IEEE 1012
	Architecture Design	Architecture Design Document	The system architecture description should include a) Generic description information; b) System overview and identification; 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.	ISO 12207/ IEEE 1016

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
			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	
		Traceability Document	Traceability between requirements specifications and architecture design	ISO 12207/ IEEE 1012

	Detailed Design	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:
			  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)
				ISO 12207/ IEEE 1016

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
		Traceability Document	Traceability between requirements specifications, architecture design and detailed design	ISO 12207/ IEEE 1012
	Coding	Source Code	• Identification of the software, including the name and date of revision and/or version, as applicable. • Source code listing	ISO 12207/ IEEE 830
		Traceability Document	Traceability between requirements and code	ISO 12207
	Testing	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.	ISO 12207/ IEEE 829
		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.	ISO 12207/ IEEE 829
		Traceability Document	Traceability between requirements specifications, architecture design, detailed design and test cases	ISO 12207/ IEEE 1012
		Test Reports	The test report should include a) Generic report information	ISO 12207/ IEEE 829

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines

			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	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.	ISO 12207/ IEEE 829
		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;	ISO 12207/ IEEE 829

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
			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.	
	Release/ Deployment	Deployment Plan	Deployment plan should include • Deployment Scope • Deployment Architecture • Deployment Strategy (roll out strategy) • Deployment Schedule • Deployment Costs • Deployment Communication plan	ISO 12207
Operation and Maintenance	User Training	Training Plan and Records	Two major audiences 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	ISO 12207/ IEEE 1219
	Operation	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	

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
			• 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. • Disaster Recovery Plan	
	User Support	Records	Problem Reports, Tickets, Resolution Records	ISO 12207
	Performance Monitoring	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)	ISO 12207/ IEEE 1219
	Maintenance	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.	
		Maintenance	Problem Reports, Change Requests, Change Records	

Stage	Phase	Deliverables/ Artifacts	Description	Recommended Standards/ Guidelines
		Records		

10.3.2 State Portal – Supporting Life Cycle Processes and Deliverables

Process	Deliverables/ Artefacts	Description	Recommended Standards/ Guidelines
Project Management	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; 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);	ISO 12207/ IEEE 1058

Process	Deliverables/ Artefacts	Description	Recommended Standards/ Guidelines
		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	
	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.	ISO 12207/ IEEE 1058
Configuration Management	Configuration Management Plan	The software configuration management plan should include a) Generic plan 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. b) Relationship with organizations such as software development or maintenance.	ISO 12207/ IEEE 828
	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;	ISO 12207/ IEEE 828

Process	Deliverables/ Artefacts	Description	Recommended Standards/ Guidelines
		3) Configuration control; 4) Configuration status accounting; 5) Configuration evaluation; 6) Release management and delivery.	
Quality Assurance	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.	ISO 12207/ IEEE 730
	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.	ISO 12207/ IEEE 1028
Content Management	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	
	Content currency report	This report should be prepared periodically (suggested once per quarter). It should contain information such as: • Summary of content change requests • Number of documents published, modified, exited • Usage analysis of various types of content Important events covered and missed	

10.3.3 State Portal - Information Security Processes

In case the organization/ facility where state portal will be hosted is not certified to ISO 27001: 2005, ISMS standard following Information security processes and relevant controls shall be subjected to audit by third party.

- Security Policy
- Asset Management
- Risk Management
- Human Resources Security
- Physical & Environmental Security
- Communications & Operations Management
- Access Control
- Information Systems Acquisition, Development & Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

10.3.4 State Portal – IT Service Management Processes

In case the IT service provider of state portal is not certified to ISO 20001: 2005 ITSM standard following IT Service Management processes as applicable shall be subjected to audit by third party.

Requirements for a Management System
- Policy
- Management Responsibility
- Documentation Requirements
- Competence, Awareness & Training

Service Delivery Process
- Service Level Management
- Service Reporting
- Service Continuity & Availability Management
- Budgeting & Accounting for IT Services

- Capacity Management
- Information Security Management

Relationship Processes
- Business Relationship Management
- Supplier Management

Resolution Processes
- Incident Management
- Problem Management

Control Processes
- Configuration Management
- Change Management

Release Process
- Release Management Process

10.4. Mapping of Roles

A list of artefacts based on the stages/ phases of the state portal life cycle has been mapped with various roles during the assignment and given in the table below.

Mapped Roles:

Stage	Phase	Deliverables/ Artefacts	Roles & Responsibility						
			Project Management Consultant	Implementation Agency	Content Service Provider	STQC	State Nodal Agency	Steering Committee	Apex Committee
Acquisition	RFP Preparation	Business Requirements	Author	-	-	-	Review	First Level Approval	Final Approval
		Detailed Project Report (DPR)	Author	-	-	-	Review	First Level Approval	Final Approval
		RFP Document	Author	-	-	Joint Review by Technical Review Team (NIC, CDAC, STQC)	Guide	First Level Approval	Final Approval
	Vendor Selection	Bid Evaluation Report	Author	Consultant	-	-	Review	First Level Approval	Final Approval
	Contract Agreement	Contract Agreement Document	Author	Consultant	-	-	Review	First Level Approval	Final Approval
	Contract Monitoring	Monitoring Reports	Author	Consultant	-	-	Monitor & Review	First Level Approval	Final Approval
Design and development	Requirements Analysis	Requirements Specifications	-	Author	-	Review	-	Approval	-
		Requirements Traceability Document	-	Author	-	Review	-	Approval	-
	Architecture Design	Architecture Design Document	-	Author	-	Review	-	Approval	-
		Traceability	-	Author	-	Review	-	Approval	-

Stage	Phase	Deliverables/ Artefacts	Roles & Responsibility						
			Project Management Consultant	Implementation Agency	Content Service Provider	STQC	State Nodal Agency	Steering Committee	Apex Committee
		Document							
	Detailed Design	Detailed Design Document	-	Author	-	Verify internal review records (at the time of acceptance testing)	-	Approval	-
		Traceability Document	-	Author	-	Verify internal review records (at the time of acceptance testing)	-	Approval	-
	Coding	Source Code	-	Author	-	Verify internal review records (at the time of acceptance testing)	-	Approval	-
		Traceability Document	-	Author	-	Verify internal review records (at the time of acceptance testing)	-	Approval	-
	Testing	Test Plan	-	Author	-	Verify internal review records (at the time of acceptance testing)	-	Approval	-
		Test Cases	-	Author	-	Verify internal review records (at the time of acceptance testing)	-	Approval	-
		Traceability	-	Author	-	Verify internal	-	Approval	-

Stage	Phase	Deliverables/ Artefacts	Roles & Responsibility						
			Project Management Consultant	Implementation Agency	Content Service Provider	STQC	State Nodal Agency	Steering Committee	Apex Committee
		Document				review records (at the time of acceptance testing)			
		Test Reports	-	Author	-	Verify internal review records (at the time of acceptance testing)	-	Approval	-
Acceptance	Acceptance Testing	Acceptance Test Plan Acceptance Test Report	-	-	-	Author (STQC)	Review	Approval	-
		Developed Solution	-	Author	-	Testing (STQC)	-	Approval	-
	Deployment	Deployment Plan	-	Author	-	Review	-	Approval	-
		Deployed Solution	-	Author	-	Audit (STQC)	-	Approval	-
Operation and Maintenance	User Training	Training Plan and Records	-	Author	-	-	Monitor & Review	Approval	-
	User Support	Reports, Tickets	-	Author	-	-	Monitor & Review	Approval	-
	Performance Monitoring	Performance Reports	-	Author	-	-	Monitor & Review	Approval	-
	Maintenance	Maintenance Plan	-	Author	-	Verify Internal Review Records	-	Approval	-
		Maintenance Records	-	Author	-	-	Monitor & Review	Approval	-
Operation	Information Security Management	Security Policy Document	-	Author	-	Audit (STQC)	-	Approval	-
		Asset Management	-	Author	-	Audit (STQC)	-	Approval	-

Stage	Phase	Deliverables/ Artefacts	Roles & Responsibility						
			Project Management Consultant	Implementation Agency	Content Service Provider	STQC	State Nodal Agency	Steering Committee	Apex Committee
	Processes	Plan & Procedure							
		Risk Management Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
		Human Resources Security Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
		Physical & Environmental Security Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
		Communications & Operations Management Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
		Access Control Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
		Information Systems Acquisition, Development & Maintenance Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
		Information Security Incident Management Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
		Business Continuity Management Plan & Procedure	-	Author	-	Audit (STQC)	-	Approval	-
	IT Service Management Processes	Policy Document	-	Author	-	Audit (STQC)	-	Approval	-
		Plan & Procedure for Service Delivery Processes:	-	Author	-	Audit (STQC)	-	Approval	-

Stage	Phase	Deliverables/ Artefacts	Roles & Responsibility						
			Project Management Consultant	Implementation Agency	Content Service Provider	STQC	State Nodal Agency	Steering Committee	Apex Committee
		• Service Level Management • Service Reporting • Service Continuity & Availability Management • Budgeting & Accounting for IT Services • Capacity Management • Information Security Management							
		Plan & Procedure for Relationship Processes: • Business Relationship Management • Supplier Management	-	Author	-	Audit (STQC)	-	Approval	-
		Plan & Procedure for Resolution Processes: • Incident Management • Problem Management	-	Author	-	Audit (STQC)	-	Approval	-
		Plan & Procedure for Control Processes: • Configuration	-	Author	-	Audit (STQC)	-	Approval	-

Stage	Phase	Deliverables/ Artefacts	Roles & Responsibility						
			Project Management Consultant	Implementation Agency	Content Service Provider	STQC	State Nodal Agency	Steering Committee	Apex Committee
		Management • Change Management							
		Plan & Procedure for Release Process: • Release Management Process	-	Author	-	Audit (STQC)	-	Approval	-