ABSTRACT

Information Technology and Digital Services Department – Formulation of Tamil Nadu Digital Transformation Strategy (DiTN) Document- Approved- Orders - Issued.

INFORMATION TECHNOLOGY AND DIGITAL SERVICE (C2) DEPARTMENT

G.O.(Ms.) No.11 **Dated: 29.03.2023**

சுபகிருது – பங்குனி – 15

திருவள்ளுவர் ஆண்டு - 2054

Read:

From the Director of e-Governance/Chief Executive Officer, Tamil Nadu e-Governance Agency letter No.AT/1/2022-COE-DeG/ TNeGA, Dated14.02.2022.

ORDER:

While moving the demand No.31, during the budget session of the Tamil Nadu Legislative Assembly held on 08.09.2021, The Honourable Minister for Information Technology and Digital Services Department has made the following announcement.

"விரைவான, கண்காணிக்கக்கூடிய, அணுகக்கூடிய மற்றும் பதிலளிக்கும் வகையிலமைந்த, வெளிப்படையான நிருவாகத்தை குடிமக்களுக்கு வழங்குவதை நோக்கமாகக் கொண்டு, மின்னாளுமையைப் படிப்படியாக அரசின் அனைத்து மட்டங்களிலும் புகுத்தி அதன்மூலம் முழுமையானதொரு அரசாங்கத்தை எய்திடும் வகையில் 'டிஜிட்டல் தமிழ்நாடு திட்டம்' செயல்படுத்தப்படும். மக்களுடன் நேரடித் தொடர்பு கொண்ட மற்றும் அவர்களிடம் தாக்கத்தை ஏற்படுத்தும் அரசுத் துறைகளின் செயல்பாடுகள் படிப்படியாக, மின்மயமாக்கப்படும்".

The Honourable Minister for Information Technology and Digital Services has also made the following announcement during the budget session on 04.05.2022.

தகவல் தொழில்நுட்பவியல் மற்றும் டிஜிட்டல் சேவைகள் துறை, வெளிப்படையான மற்றும் குடிமக்களை மையப்படுத்திய அரசாங்கத்தை வழங்குவதற்கான தொலைநோக்குப் பார்வையுடன், அனைத்துத் துறைகளும் தங்கள் செயல்பாடுகளை டிஜிட்டல் மயமாக்க உதவுவதை தனது நோக்கமாகக் கொண்டுள்ளது. அனைத்துத் துறைகளும் தங்களது முக்கிய செயல்திறன் குறிகாட்டிகள் (Key Performance Indicators) மற்றும் விளைவுகளை (Outcomes) எட்டுவதற்கு தமிழ்நாடு டிஜிட்டல் மயமாக்கல் வியூகம் (DiTN) உதவும். மேலும், தமிழக மக்களுக்கு விரைவான, கண்காணிக்கக்கூடிய, அணுகக்கூடிய, பதிலளிக்கக்கூடிய மற்றும் வெளிப்படையான (SMART-Swift, Monitorable, Accessible, Responsive and Transparent)

நிர்வாகத்தை வழங்கும். தமிழ்நாடு டிஜிட்டல் மயமாக்கல் (DiTN) வியூகம், டிஜிட்டல் முதிர்ச்சியை மதிப்பிடுவது முதல் தகவல்தொழில்நுட்ப வியூகத்தைச் செயல்படுத்துவது வரையிலான அனைத்து வழிகாட்டுதல்களையும் வழங்கும்.

தமிழ்நாடு டிஜிட்டல் மயமாக்கல் (DiTN) வியூகம், தகவல் தொழில்நுட்பத் திறனை ஒவ்வொரு துறைசார் அலுவலகத்திலும் உருவாக்குவதை நோக்கமாகக் கொண்டுள்ளது. அனைத்து விதமான தகவல் தொழில்நுட்பத் திறன் பெற்ற மனித வளத்தைக் கொண்ட ஒரு "துறைசார் டிஜிட்டல் யூனிட் (Departmental Digital Unit - DDU)" ஒவ்வொரு துறைசார் அலுவலகத்திலும் ஏற்படுத்துவதன் மூலம் இந்நோக்கத்தை எய்திட முடியும். இதற்கான நபர்கள், தமிழ்நாடு மின்னாளுமை முகமையால் வெளிச்சந்தையில் இருந்து தெரிந்தெடுக்கப்பட்டு, ஒவ்வொரு துறையிலும் சமஊதிய நிர்ணயம் கொண்ட ஒப்புவிக்கப்பட்ட நிரந்தரப் பணியிடங்களுக்கு மாற்றாகப் பணியமர்த்தப்படுவர்.

தமிழ்நாடு டிஜிட்டல் மயமாக்கல் (DiTN) வியூகத்தின் நோக்கங்களை எய்திடும் வகையில் மின்னாளுகைத் திட்டங்களைச் செயல்படுத்துவதற்குத் தேவையான வரவு-செலவுத் திட்ட ஒதுக்கீடு, ஒவ்வொரு துறைக்கும் ஏற்படுத்த முன்மொழியப்பட்டுள்ளது.

2. Accordingly, the Director of e-Governance / Chief Executive Officer, Tamil Nadu e-Governance Agency (TNeGA) has formulated a Tamil Nadu Digital Transformation Strategy Document for the State of Tamil Nadu and requested the approval from Government for the Tamil Nadu Digital Transformation Strategy (DiTN) Document.

3. The Tamil Nadu Digital Transformation Strategy (DiTN) Document has been carefully crafted keeping three key pillars in view:***Connected Citizens; Digital Economy; and Transformed Services***.

4. The Tamil Nadu Digital Transformation Strategy (DiTN) document will improve efficiency & effectiveness of Tamil Nadu Governance and Administration. The 'DiTN' as a strategy document is first of its kind for the State of Tamil Nadu, designed keeping in view the existing and upcoming policies, procedures and systems, for improving the service delivery for digital governance and Government. This strategy document acts as a guidance to State Departments in drafting their own digital transformation strategy and its implementation.

5. Some of the salient features of the Tamil Nadu Digital Transformation Strategy (DiTN) Document are as follows:

- Aiming for the transformation for better accessibility, transparency, efficiency, and accountability to the Citizens and Government Departments, by making contactless, paperless and presence-less governance.

- Focus on strengthening the ecosystem and developing the talent pool and incubation centers to make the State a hub for innovation and entrepreneurship.

- To further strengthen the process of digitalization in Tamil Nadu, to empower Citizens with the required digital infrastructure across the State including remote locations.

- To enhance digital connections with Tier-II and Tier-III towns by ensuring Governmental services are available to Citizens conveniently – through apps, websites, kiosks, etc.

- Focus on developing a conducive ecosystem for disruptive technologies and provide incentives for Governmental adoption to improve G2B and G2C service delivery.

- Focus on developing a digital ready workforce by training college graduates; Upskilling Government staff and citizens of the State.

6. The successful achievement of the Digital Transformation Policy will depend on an integrated approach during implementation supported by developing strategic synergies and partnerships. The Digital Transformation shall have following Governance framework.

Apex IT committee (APC)

The Apex IT committee (APC) would provide strategic guidance to the overall State digitalization program. APC will provide for policy and monitoring, guidance, leadership, prescribe deliverables and milestones. It will evaluate periodically and direct the DiTN Monitoring Committee (DMC) to take remedial actions if any.

The Apex IT committee shall be chaired by the Hon'ble Chief Minister, with Minister for Information Technology and Digital Services, Minister for Finance and Human Resources Management, Chief Secretary, Additional Chief Secretary, Finance, Principal Secretary (I) to Hon'ble Chief Minister as members. Other Departmental secretaries whose projects are being reviewed shall be invitees. Secretary, (Information Technology and Digital Services) shall be the member secretary of Apex IT Committee.

The key roles and responsibilities of Apex IT Committee include:

- Provide visionary and catalysing leadership at the highest level of Government to Support the implementation of the Policy
- Provide guidance and direction to all Departments in execution of its mandate;
- Set the IT vision for the State; and
- Provide strategic guidance to DiTN Monitoring Committee.

DiTN Monitoring Committee (DMC)

The DiTN Monitoring Committee would drive the State-wide implementation of DiTN. It shall review and monitor the progress of Digital Tamil Nadu implementation based on Apex IT Committee decisions. It shall be chaired by the Chief Secretary with Secretary (Information Technology and Digital Services) as its Member Secretary. Additional Chief Secretary, Finance, Secretaries of the respective Departments who are digitalizing their operations will be members, along with Chief Technology Officer (CTO) of Information Technology and Digital Services Department and the Director of e-Governance/Chief Executive Officer, Tamil Nadu e-Governance Agency, and members of the State Project Monitoring Unit (SPMU).

All e-Gov projects of all Departments shall be brought to the committee for monitoring, guidance, review, and recommendation. It shall also pursue with Departments to take up relevant e-Gov projects which are the priority of the Government. However, for approval of e-Gov/IT projects, the existing process of approval and circulation through Information Technology and Digital Services Department and Finance be followed. It shall also ensure resolution of project difficulties including inter-Departmental issues during project execution.

It shall, as required, review all major IT projects being implemented in the State to ensure an integrated approach. This committee would drive the architecture design and roll out for select sector/Departments along with the Departmental stakeholders. Its main role will be to ensure synergy among various e-Governance/ IT initiatives proposed for or by the respective State Departments and ensure uniformity of design and standards across Departments.

The key roles and responsibilities of DiTN Monitoring Committee include:

- Integrate the structural requirements of DiTN across all Departments;
- Improve selection and use of new technologies for implementation of the policy;
- Synergise and rationalize DiTN Implementation across all Departments;
- Setup of Digital transformation across the State; (Architecture, Infrastructure, Application, etc.)
- Approve Policy/Orders/Instructions relating to implementation of DiTN;
- Review e-Gov / hardware procurement progress of all Departments.
- Coordinate across all State Departments for e-Governance/ IT initiatives;
- Oversee implementation activities.
- Resolve conflicts arising out of implementation related activities.
- Review and issue instructions on Departmental digitalization initiatives which are functioning without any integration with other systems.
- Ensuring that good governance principles are applied and adhered to in the implementation of the Policy;

State Project Management Unit (SPMU)

TNeGA will function as the State Project Management Unit (SPMU) to provide functional, technical and managerial inputs to the DiTN Monitoring Committee. The Chief Technology Officer (CTO) of Information Technology and Digital Services Department will oversee all IT projects being implemented through TNeGA.

The Key roles and responsibilities include:

- To provide support to all Departments to steer and anchor the policy implementation initiatives;
- To support the DiTN Monitoring Committee in all its initiatives with policy and implementation related issues and new initiatives necessitated;
- To support Departments in crafting progressive e-Governance strategies, to promote SMART- Swift, Monitorable, Accessible, Responsive and Transparent Governance;
- To promote innovation and evolve models for empowerment of citizens through the policy initiatives and to promote participatory governance;
- To develop a statistical strategy for measuring the goals of this policy and also to create appropriate data sources;
- To put in place an institutional mechanism for capacity building of all Department and its agencies, including assessment and evolution of suitable training packages/modules for capacity building to enhance competitiveness for successful implementation of the policy including to cut on cost and time over run;
- Coordinate with all the State Departments to identify the vision/ mission statements, their short, medium, and long-term e-Governance and IT initiatives/plans;
- Perform and support necessary support - related activities under DiTN implementation of the architecture for all Departments and Agencies;
- Support on maintenance of IT infrastructure assets in Departments, functioning with hi-tech labs;
- Provide technical assistance in designing e-Governance/ IT initiatives across State Departments/ Agencies;
- Provide project implementation support to State Departments/ agencies during development and implementation of e-Governance/ IT initiatives;
- Facilitate design and roll out of Single Sign on (SSO) mechanism for all Departments; and Communicate and share information amongst stakeholders for efficient implementation;
- Implement the directions of DiTN Monitoring Committee (DMC); and
- Submit periodic status reports to DiTN Monitoring Committee (DMC) on the progress of implementation of e-Governance/IT initiatives at State Departments/ Agencies.

Departmental Project Monitoring Unit (DPU)

Each Department executing an e-Government program/ IT initiative will have a dedicated Departmental Project Monitoring Unit (DPU). The Departmental Project Monitoring Unit will comprise of the Officer responsible for the project in the Department; functional technical/ IT consultants available in the Department; the IT cadre resources (nominated by TNeGA); and the designated Data officer of the Department. The Departmental Project Monitoring Units shall administratively be controlled and report to State Project Management Unit.

The inhouse team at Department level shall be responsible for the Department's digital initiatives/ interface for the rollout of DiTN. Whenever additional skill sets are required for the Department, the same will be made available by TNeGA/ELCOT. Considering the fast-paced development of IT and Technology applications, a healthy mix of outsourced, contract, and timescale employees shall be maintained.

The Key roles and responsibilities will include:

- Coordinate with State Project Monitoring Unit for technical, functional, financial requirements for designing, developing, and implementing Department level e-Governance/ IT initiatives;
- Prepare Department level Digital Governance/ transformation strategy;
- Draft vision, mission and objectives of the Department in improving service delivery;
- Consolidate and analyze the list of services offered by the Department;
- Consolidate and analyze the list of IT applications/ systems currently used by the Department for the service delivery;
- Support each Department to have single portal pertinent to schemes, progress and project management. Conduct feedback surveys to understand the issues faced by the citizens and businesses and their requirements to improve service delivery;
- Develop implementation plan and cost estimates for the proposed recommendations;
- Preparation of Tender documents and carrying out bid process management to bring the system integrator/ consultants on board to develop the proposed systems and policies;
- Periodic evaluations of the projects/ programs and take-up corrective measures during the implementation; and
- Conduct mid-term and End-term project/ program evaluations to report the achievements and lessons.

7. The Government, after careful examination, hereby accord approval to the "Tamil Nadu Digital Transformation Strategy" (DiTN) document which will enable the Government of Tamil Nadu to SMART-Swift, Monitorable, Accessible, Responsive and Transparent Governance.

8. A detailed booklet containing the Tamil Nadu Digital Transformation Strategy (DiTN) Document is annexed to this order.

9. The Director of e-Governance/ Chief Executive Officer, Tamil Nadu e-Governance Agency shall provide support to all Departments to steer and anchor the policy implementation initiatives and submit periodic status report to DiTN Monitoring Committee (DMC) on the progress of implementation of e-Governance /IT initiatives of State Departments/ Agencies based on Tamil Nadu Digital Transformation Strategy (DiTN) Document.

(By Order of the Governor)

J. KUMARAGURUBARAN
SECRETARY TO GOVERNMENT

To
All Departments of Secretariat, Chennai 600 009.
All Heads of Department.
All District Collectors/ District Magistrates.
The Director of e-Governance / Chief Executive Officer,
Tamil Nadu e-Governance Agency, Chennai – 600 002.
The Managing Director (FAC), ELCOT, Chennai – 600 035.
The Director (FAC), Tamil Virtual Academy, Chennai – 600 025.
The Managing Director, Tamil Nadu Arasu Cable TV Corporation Limited,
Chennai – 600 002.
The Managing Director, Tamil Nadu FibreNet Corporation Limited, Chennai - 600 002.
The State Informatics Officer, National Informatics Centre, Chennai – 600 090.

Copy to:

The Principal Secretary-I to Hon'ble Chief Minister, Secretariat, Chennai – 600 009.
The Chief Minister's Office, Secretariat, Chennai – 600 009.
The Senior Personal Assistant to Hon'ble Minister for Finance & Human Resource Management, Secretariat, Chennai – 600 009.
The Senior Personal Assistant to Hon'ble Minister for Information Technology and Digital Services, Secretariat, Chennai – 600 009.
The Private Secretary to Chief Secretary to Government, Secretariat, Chennai – 600 009.
The Senior Private Secretary to Additional Chief Secretary to Government, Finance Department, Secretariat, Chennai – 600 009.
The Private Secretary to Secretary to Government, Information Technology and Digital Services, Secretariat, Chennai – 600 009.
The Resident Audit Officer, Secretariat, Chennai – 600 009.
The Content Creator (MS)/Moderator (MS)/Nodal Officer (MS), Information Technology and Digital Services, Secretariat, Chennai – 600 009. (with a request to host the G.O. in the Government website)
SF/SC.

// Forwarded / By Order //

Section Officer

Table of Contents

List of Tables

List of Figures

Disclaimer

Vision Statement

1 Vision for Tamil Nadu Digital Transformation Strategy

The Digitalization of Governance and Private Sector has picked up pace over the past five years and predominantly during the COVID-19 pandemic. Government of Tamil Nadu now aims to start a new journey of transforming governance.

- ✓ *Time bound State Digital Transformation Journey*
- ✓ *CCOVID-19 resilience & digital embracement learnings*
- ✓ *Alignment with Digital India's Blueprint*
- ✓ *Measure, Grow & Innovate*

One of such initiatives is the roll-out of e-office in the state with an objective towards paperless government. The Government has announced two other programs towards digitalization of government processes – Tamil Nadu Digital Transformation Strategy (DiTN) and Tamil Nadu Decision Support System (DeTN)**.** DiTN aims at transforming the Government processes by deploying digital technology, while the DeTN aims at improving decision and policy making in government departments.

This document is an effort to articulate the DiTN strategy and to act as a guide for all departments to design, develop and implement digital transformation programmes and projects to achieve the vision of statewide digital transformation.

The mission of the Information Technology & Digital Services Department, Government of Tamil Nadu is to help all departments transform their government services and functions and make the Government digitally driven with a vision to provide transparent and citizen-centric government, thus providing a "**Digital Governance for the State of Tamil Nadu**".

The DiTN will thus help departments convert their Key Performance Indicators (KPI) and the outcomes into a technological architecture that will support their own vision. The DiTN vision comprises of three pillars to ensure a "Whole of Government" approach: Connected Citizens, Digital for economy and Transformed services.

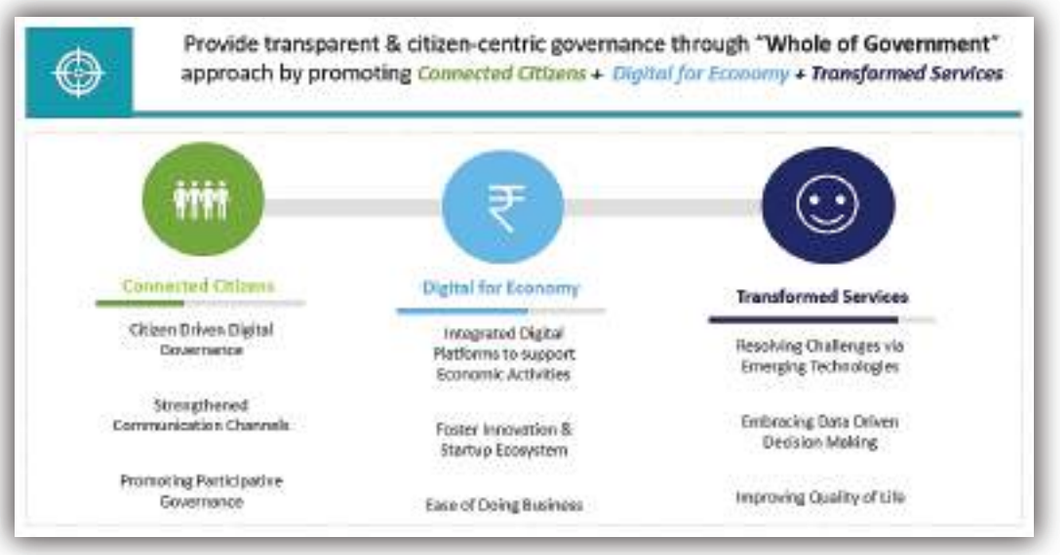
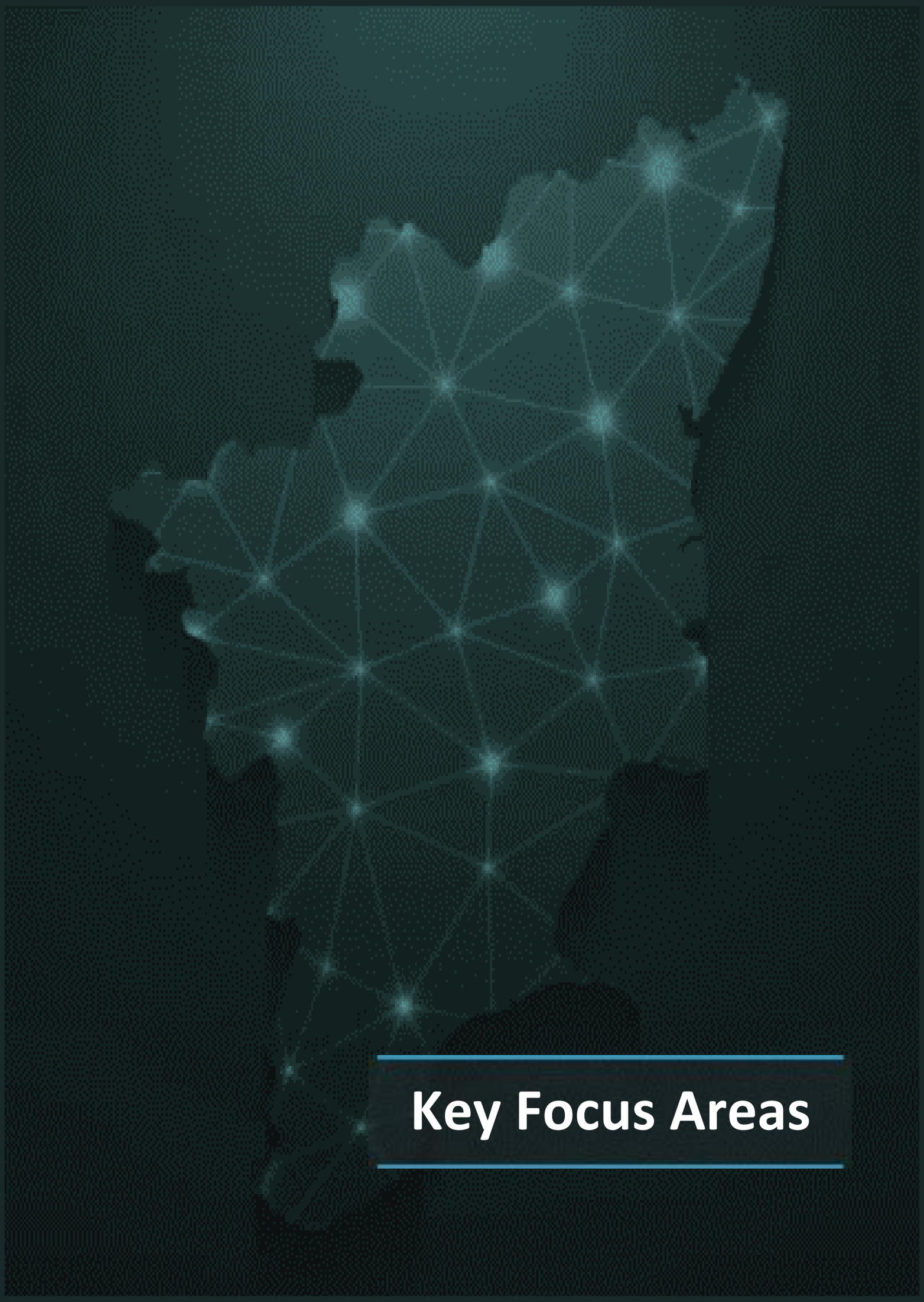


Figure 1: Vision for Digital Governance for the State of Tamil Nadu

The vision for "Digital Governance for the State of Tamil Nadu" envisages creating access to all services to citizens in their locality, through a digitally unified service delivery channel, thereby ensuring transparency, security and reliability of services.

Table 1: Three key pillars of the vision

 **Connected Citizens**	Promote citizen driven governance model with '*Tamil First and Voice First*' to ensure equitable access to quality public information and services conveniently for all citizens across all social and economic strata. It will encompass new-age experience while empowering citizens to manage, access and control their data. Government shall provide adequate communication platforms to engage and promote citizen participation in governance while ensuring timely redressal of grievances.
 **Digital Economy**	Support economy by providing necessary digital tools and platforms to foster digital payments and encourage innovations that can lead to fundamental transformation and catalyze growth and employment opportunities. The thrust will be on digital ecosystems to promote Government-to-Business (G2B) service delivery, thereby improving the 'Ease of Doing Business' to enhance investment potential in key focus sectors. Considering the idea of data as a public good, the Government will make efforts to make electronic data public to the extent possible and consider data monetization for revenue generation, subject to maintaining data privacy. The IT systems should generate data, information and provide infrastructure services leveraging open, interoperable, standards-based digital systems. This will also enable the private sector to offer value added services based on the publicly available data.
 **Transformed Services**	Develop a statewide digital e-Governance services ecosystem that supports citizen needs and provides coverage in a transparent, inclusive, and affordable way. Provide proactive governance leveraging the strength of emerging technologies including block chain, AI based predictive data analytics and a unified beneficiary database. Transformed services ease service delivery and attempt to improve the overall quality of life of its citizens.



Key Focus Areas

2 Key Focus Areas

The Information Technology & Digital Services Department, Government of Tamil Nadu (IT&DS) aims to focus on the following areas to achieve the vision statement of "Digital Governance for the State of Tamil Nadu".

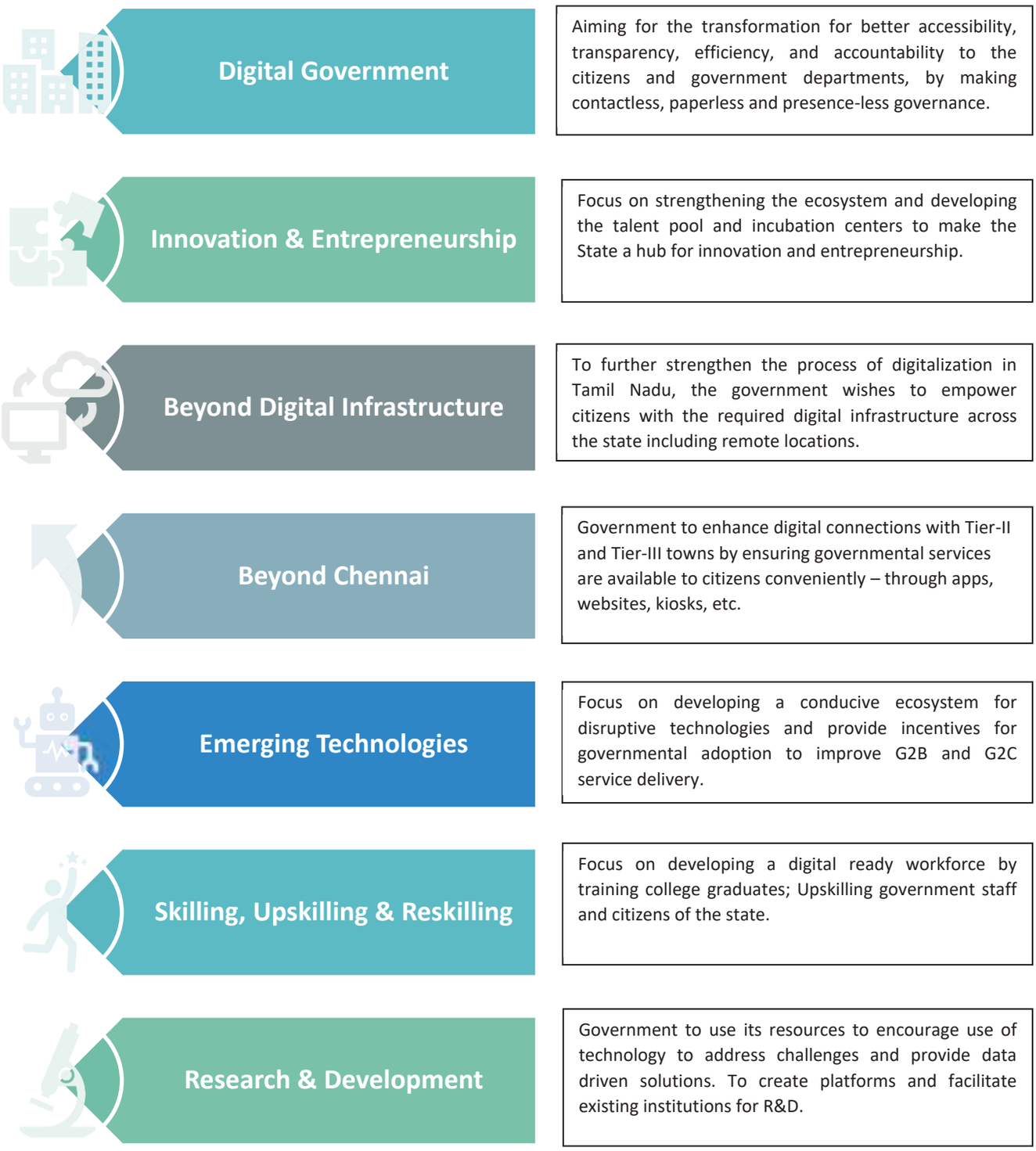
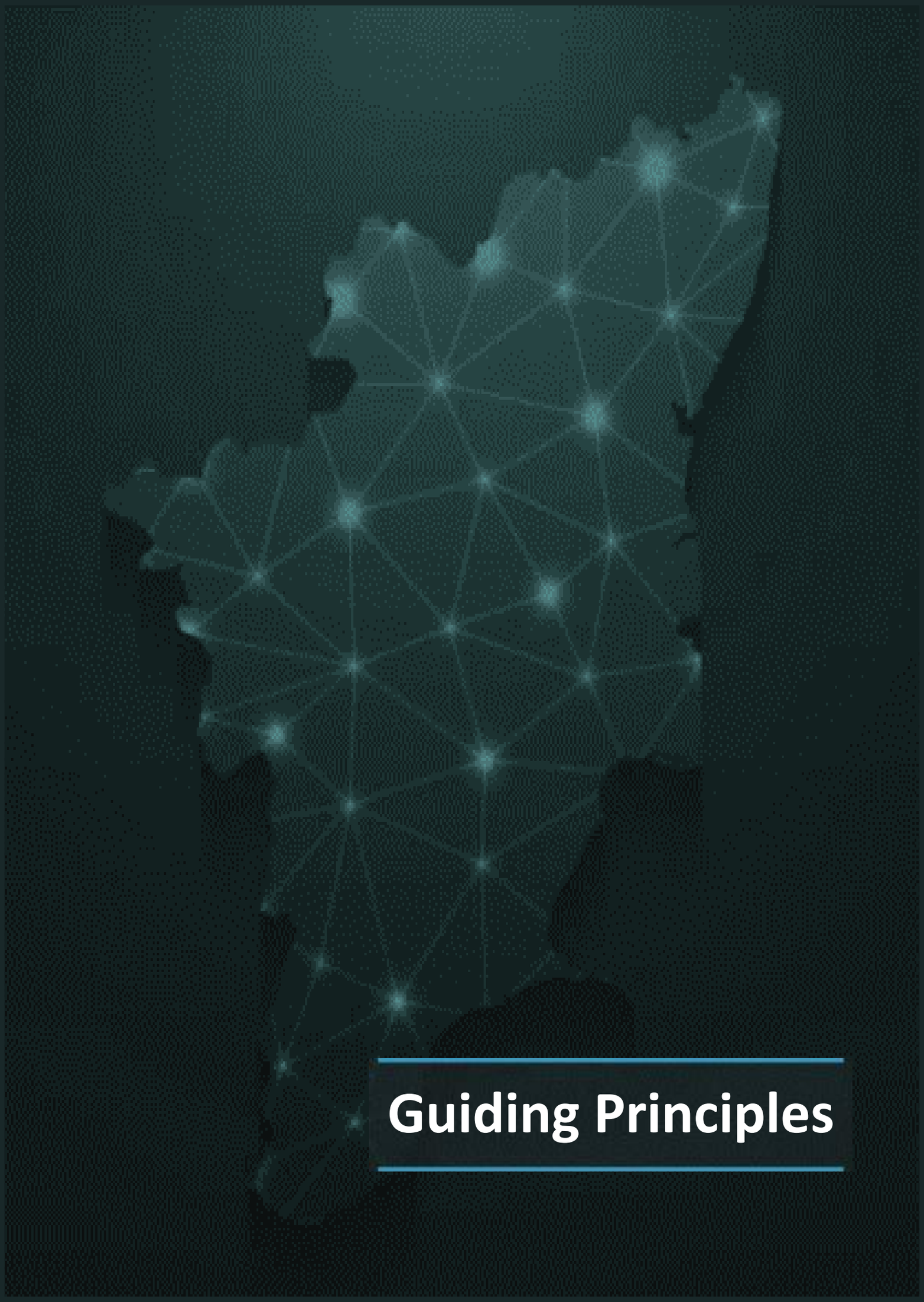


Figure 2: Key Focus Areas



Guiding Principles

3 Guide to Develop Digital Transformation Strategy

To develop a comprehensive and cohesive DiTN across all departments it is important to follow a common structured approach for all departments. The guiding principles for design, development, and implementation of the DiTN are divided into eight considerations. These should be kept in mind by each department while drafting their own DiTN strategy:

Figure 3: Guiding principles for the Digital Transformation Strategy

Each of the guiding considerations are described below:

3.1 Citizen-centric/human-centric considerations

Citizens are key consumers of Government services and the expectations of citizens are influenced by their experiences and interactions in multiple environments. In the private sector, successful businesses adopt a customer-centric approach to provide better experiences for their customers and make them more loyal to their product or services. User friendliness and personalization of services is one of ways how the businesses attract and retain the customers. Governments services are often designed around generic requirements and procedures rather than the requirements of users. Adopting a human-centered design allows adopting human perspective in all steps of the problem-solving process. The user-oriented framework will rely heavily on user participation and user feedback in the entire planning process. By adopting a citizen centric and human centric approach in designing and delivering services, departments can aim to deliver greater citizen satisfaction. Departments can measure the citizen satisfaction through various mechanisms and use that to improve the service design and delivery.

3.2 Performance Metric Consideration

Performance Metric will act as a guiding principle to help achieve specific and measurable goals for the departments. This will be determined by the overall government or/ and department level policies, support systems and the focus areas listed in this document. Performance measurement will flow from identifying qualitative and quantitative KPI, for each service and function for every department.

3.3 Business Functions Consideration

Various departments are providing multiple services and perform different business functions in achieving their objectives. The departments should identify the current state of functions and services, then identify services and functions for rationalization and Business Process Re-engineering (BPR).

The BPR exercise involves review of the various processes for all existing services in departments; identify key challenges; conduct best practices evaluation; and derive the 'to-be' scenario (where they want to be in future) and finalize the 'to-be' designs for each of the service and function.

Subsequently, departments shall draft a plan for implementing the re-engineered services. A maturity Vs. value (2x2 matrix - High and Low in both axes) be used for prioritization the of re-engineering processes, to follow a staggered implementation approach.

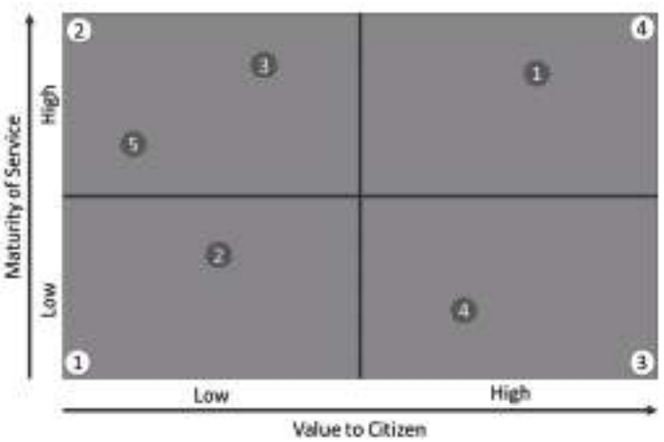


Figure 4: Service maturity and prioritization framework

Services with High value to citizens and delivered completely online are to be placed in the right top quadrant (4), whereas the service with high value to citizen but delivered in a manual mode to be placed in the right lower quadrant (3). The departments should give priority to services in quadrant 3 where all priority services are delivered in manual mode but offer high value for undergoing BPR and the Digital transformation.

3.4 Integration across services/departments consideration

Integration of systems for services and functions offered by departments should be a key element while drafting the department level DiTN. Integration can be at two levels: Integration of systems, applications and databases within the department and across departments. For the services and functions under the purview of any department, it is important to have an integrated and single source of truth for all the data. It is essential that all systems and databases pertaining to services and functions are streamlined to avoid duplication of data collection, analysis and management. As the DiTN aims to digitize governance and administrative mechanisms, benefits can be visualised when departments

work together towards developing a single or common portals/ dashboards and exchange data between them.

3.5 Application/Systems Consideration

"Application" guides the departments to craft a blueprint for the IT systems deployed their interactions and relationships with government services, functions and existing applications/ systems. It defines the strategy behind implementing IT systems in the State IT eco-system, listing out the inventory of existing systems and chalking out a transformation plan, in line with the Tamil Nadu State Level Enterprise Architecture (TNEA) as detailed in Chapter 4. The process of revisiting the department level systems and applications will involve:

- ✓ Identifying the systems and the current state of maturity and utility and to align the same with BPR as detailed in section 3.2.
- ✓ Identifying system level gaps against future state department level application architecture for each system/application; and
- ✓ Developing an application transformation plan for each of the systems and aligning the same with department level application architecture and TNEA.

The following are the key elements for the application architecture design:

- ✓ Standards and regulations as listed in Annexure 6.2;
- ✓ Architectural, design and operational recommendations as listed in Annexure 6.3; and
- ✓ Architecture approach as listed in Annexure 6.5.

3.6 Data consideration

Data and its management are the most important differentiators to provide best-in-class services to citizens and businesses. Data as a guiding principle should ensure seamless information flow within and across departments and relevant external stakeholders. It connects and integrates all departments at data layer, facilitating increased collaboration among departments/agencies. It also keeps the security and technical requirements of individual data elements. The approach to be adopted for data management during process redesign and system improvements/ development are:

- ✓ Identify the current data elements in use (digital or manual);
- ✓ Identify data usage requirements;
- ✓ Develop data digitization strategy;
- ✓ Identify Data architecture;
- ✓ Map the data usage requirements to architecture; and
- ✓ Develop the future state data architecture.

The following are the key elements for data architecture designs:

- ✓ Mandatory Standards listed in Annexure 6.2 and 6.3; and
- ✓ Open Data standards listed in Annexure 6.2 and 6.3.

3.7 Technology Consideration

Technology to be adopted as a guiding principle; that defines the principles, methodology, design, and guidelines for implementation of the IT infrastructure. It includes all activities to design and implement better technology architecture for Digital Tamil Nadu and provide easy and seamless access to ICT infrastructure for departments to operate. The steps to be followed while drafting the department level digital transformation strategy are:

- ✓ Review of As-Is Tech architecture, (if any);
- ✓ Assess the emerging and impactful technology domains;
- ✓ Identify technology gaps and mitigation strategy;
- ✓ Develop future state technology architecture; and
- ✓ Develop the technology architecture transformation plan.

The following are key to the technology architecture design:

- ✓ Technology independence;
- ✓ Open standards;
- ✓ Shared infrastructure;
- ✓ Micro-Services strategy;
- ✓ Cloud Strategy; and
- ✓ Resilient infrastructure[1].

3.8 Security Consideration

Digital transformations linked to online services open-up multitude of threats. It is strategically important to define and implement policies, processes, and controls for ensuring information security. Security cannot be confined at a single point or level. It needs to be addressed at all levels. The departments need to consider the following steps while drafting their digital transformation strategy -

- ✓ Assessing the current Security Architecture;
- ✓ Defining the present and future security requirements;
- ✓ Assess the impact of emerging technologies to security as threats and opportunities;
- ✓ Develop the future Security Architecture; and
- ✓ Develop the Security Architecture Transformation plan.

[1] redundancy and no single point of failure

The following are key to security architecture design:

- ✓ Data Integrity;
- ✓ Data Privacy & Confidentiality;
- ✓ Data Availability;
- ✓ Secure by Design; and
- ✓ Regular threat vulnerability assessments.

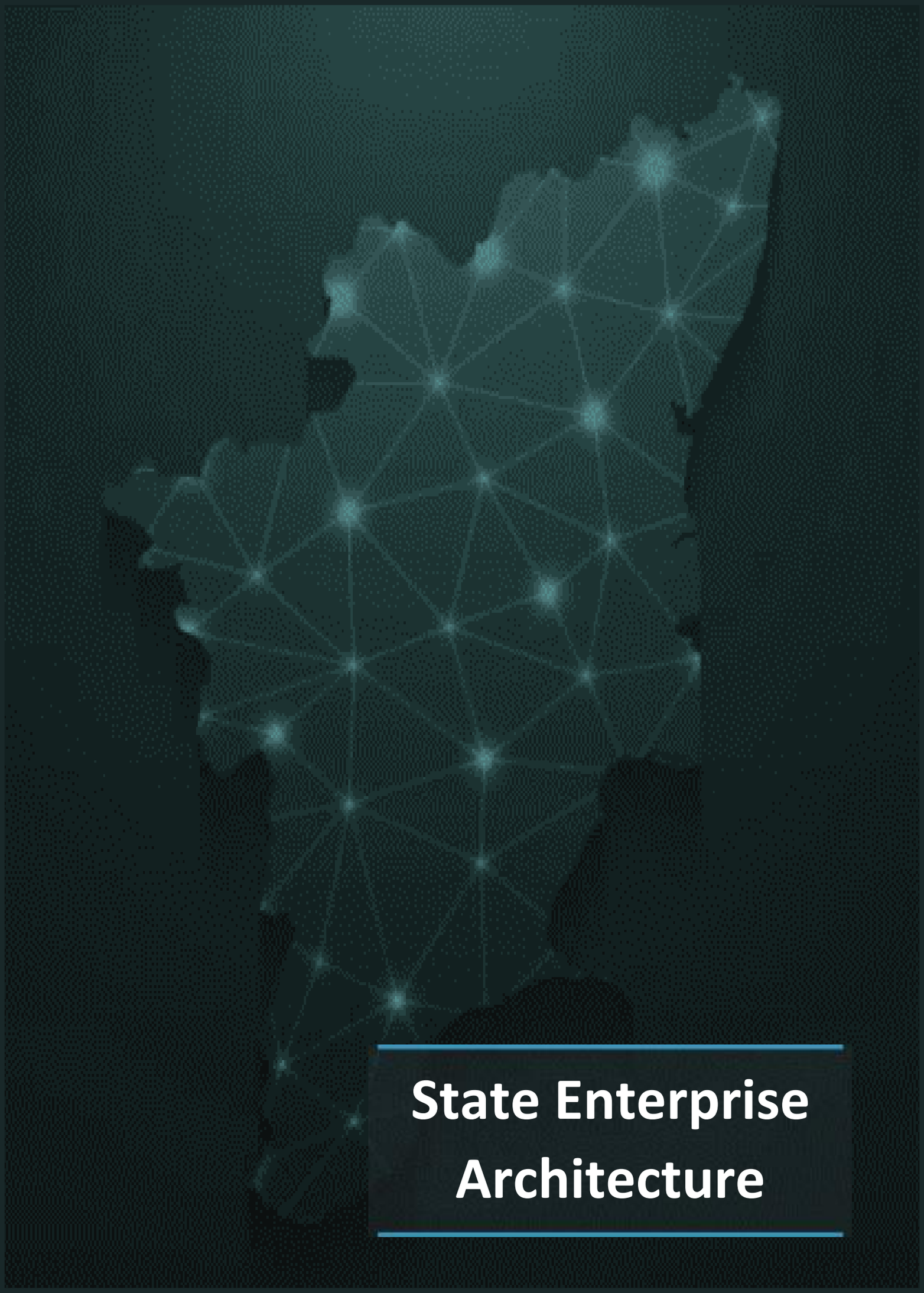
3.9 Socio-political consideration

The socio-political considerations will help the departments design digital systems that are easily accessible to all and not create any new divide with the digital divide being a prominent one. The spread of internet has created multiple communication channels and social media platforms that help reach out to people in a simple, efficient manner. However, the same also poses a threat of misinformation spreading easily. Departments have to navigate through the challenges and chose the right platforms with sufficient checks and balances. The emerging technologies allow use of Artificial Intelligence (AI) and automation to design services efficiently and help in reduction of biases of underlying data, through use of machine learning.

3.10 Governance Consideration

The Governance consideration will guide departments in development, management, and realization of requirements for DiTN. It is important to adopt good governance best practices and the framework, else it may result in non-standardized technology / product selection / purchasing / development, leading to siloed applications and efforts. This will result in duplicity and inefficient use of resources. A poor governance framework will have a long-term financial and operational impact and will create problems in integration, collaboration, and standardization.

Effective governance structure ensures that priorities are based on broad consensus across the departments. It is, however, not a one-time responsibility, nor is it limited to specific projects but an iterative and continuous process. The departments must consider setting up of a governance structure for digital transformation and align to the state governance framework. Refer section 5.2. for more information.



State Enterprise Architecture

4 Tamil Nadu State Level Enterprise Architecture

Tamil Nadu State Level Enterprise Architecture (TNEA) is the reference enterprise architecture framework for Government IT applications and services delivery. TNEA postulates minimal architecture with citizen at its core and creates a 24x7 digital services delivery ecosystem for the government. The vision for DiTN strategy is broadly aligned to the India Enterprise Architecture's (IndEA) Minimum Viable Architecture.

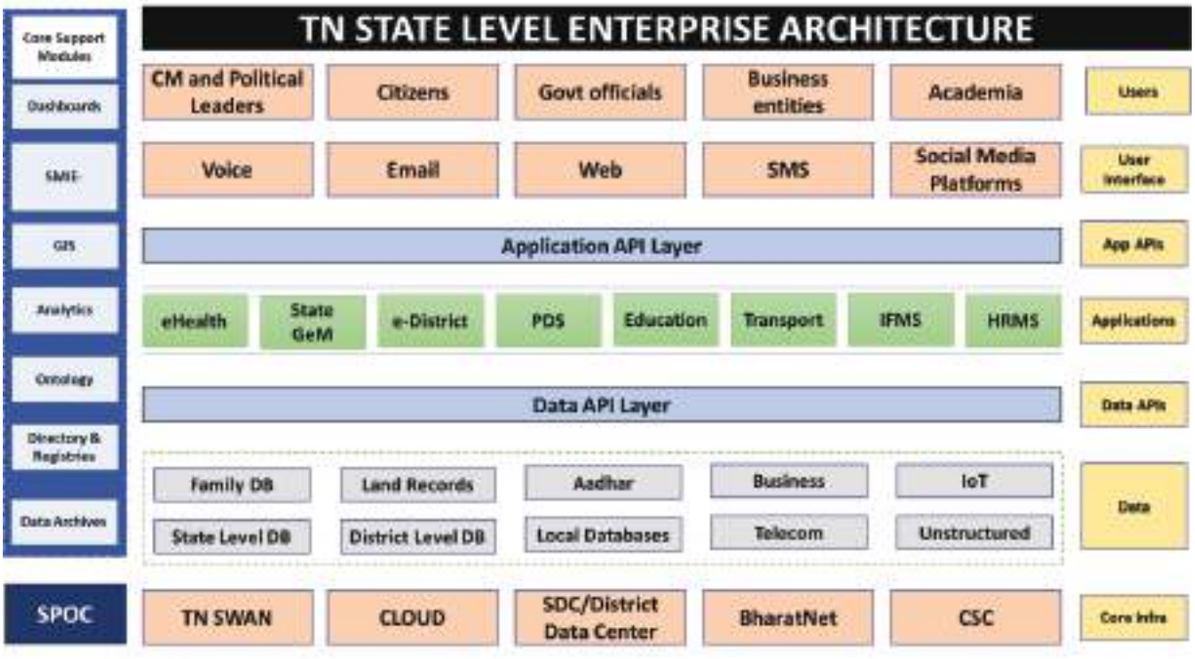


Figure 5: Tamil Nadu State Level Enterprise Architecture (TNEA)

The TN-State Level Enterprise Architecture (TNEA) shall deliver all services to the citizen (G2C) via different user interfaces through proper consent gateway. The user establishes direct connect with departments where the Government can deliver services in a defined time. Even G2B/ Enterprise services shall be rendered using the same architectural framework supported by Application Programming Interface (API) services and integration.

The **TNEA consists of four layers** – Core infrastructure, Data, Applications, and User interface/access layers.

- **Core Infrastructure layer** consists of computing infrastructure to host data and applications supported by networks for connectivity;
- **Data layer** envisaged is in line with federated data structure with State, district and local databases in addition to the functional / departmental databases like family, land, and Public Distribution System (PDS). This plays a critical role in standardizing user data, facilitating integrated services delivery, supporting data analytics and enabling predictive services. The Unique Digital ID will help in rendering predictive services without citizens having to apply for services.
- **Application layer** provides multiple ICT solutions and tools designed to render various Government services.

- **User Interface layer** ensures citizen service delivery across multiple channels seamlessly. In addition, API layer both at data and application levels enables integrated services with improved turnaround times. API layer can also facilitate data exchange and services integration required with other service providers, including all business services.

The Core Support Modules like Dashboards, GIS platform, Analytics, Identity and Access Management, Directories and Registries fulfil certain basic functionalities required for all departmental ICT applications and can be extended as a service.

By adopting **TNEA**, we can achieve the following:

- ✓ Directory of Services in Service Dashboard with Single Sign-on authentication;
- ✓ Simplification in Service Delivery - Contact-less, Paper-less, Cash-less services;
- ✓ Gap Infrastructure deployment, Scaling and up-gradation of the existing solution;
- ✓ Framework/rule-based approach to building applications;
- ✓ Security Compliance with Interoperability and Migration;
- ✓ Reuse of Data Created by Original Source Department – Data Exchange and Analytics; and
- ✓ Re-structuring of legacy systems to be in line with TNEA defined Principles, Standards, standards roles and responsibilities.

4.1 Principles of TNEA

The key goals of the TNEA can be classified into domain and technology perspectives:

- ✓ **Domain**: maximum service coverage, inclusiveness, security and privacy by design, education and empowerment of citizens and
- ✓ **Technology**: building blocks, interoperability, a set of registries as single sources of truth, open standards, open APIs and above all, a minimalistic approach.

The following principles will be adopted for the detailed design of TNEA to achieve the above goals:

- ✓ Citizen to control 'processing of personal data' (Consent Gateway);
- ✓ '*Tamil First and Voice First*' to drive inclusivity;
- ✓ Digital services data and applications will be hosted at State, District and Local levels following the principle of minimality at each level;
- ✓ Citizen data will be held at the lowest level consistent with the needs of the application;
- ✓ Systems of Record at State level will hold the primary data. All other IT systems or applications will have access via links, subject to applicable permissions and consent (e.g., role-based access and privileges);
- ✓ Large facilities and government departments may store, process and handle their data. Small facilities that do not have the capacity/ infrastructure can resort to licensed data repositories;

- ✓ The data fiduciary (Tamil Nadu e-Governance Agency (TNeGA) will manage / process the data and be responsible for data protection and compliances under the applicable laws and TN Data Policy 2022; and
- ✓ Data Privacy and Security shall be fundamental in all applications / service design.

4.2 Strategic building blocks for TNEA

Strategic building blocks are reusable frameworks one can rely upon for designing, developing and delivering the services and functions. This document has identified the minimum viable set of building blocks required.

IT&DS department is working towards the design, development and establishment of these building blocks, to achieve the TNEA and the State departments to align their digital transformation strategy to the State Level Enterprise Architecture to achieve the unified digital transformation.

IT&DS department is also exploring utilizing the emerging technology led governance solutions, with focus on fourth industrial revolution, Data analytics, Artificial Intelligence, Machine Learning, Drones, Augmented Reality, Virtual Reality and Blockchain. These initiatives will complement TNEA and be available for the State departments to utilize and include them as a part of their digital transformation strategy.

The following section lists key initiatives that departments can leverage upon to:

- ✓ *Complement and support department level digital transformation of services and functions;*
- ✓ *Avoid developing systems/ applications, procedures, and databases working in silos;*
- ✓ *Align with TNEA; and*
- ✓ *Meet the overall vision and focus of DiTN.*

The following are the strategic building blocks for TNEA and current/ upcoming initiatives at the State level that departments should leverage and plan for integration with:

4.2.1 Secure Statewide Network

BharatNet and National Optic Fibre Network (NOFN), which envisages highspeed connectivity will form the basis of the core network. End to end security through HTTPS and SSL will be used in all communications. For sensitive applications and data, strong end-to-end encryption including quantum security to be used. For specific applications like Telemedicine, e- Education, e-agriculture, e-Health, e-finance etc. that requires fast and robust data links, there is a need to specially design networks with low latency and high bandwidth. Development of 5G corridors will be examined and pursued.

4.2.2 Security and Privacy Operations Centre (SPOC)

All Digital Services-Cloud and the Digital Services Network events is required to be under 24x7 security surveillance. This is to be achieved by establishing a Security Operations

Centre (SOC). Establishment of a dedicated Privacy Operations Centre (POC) will help drive compliance to the privacy requirements. The SPOC can have role-defined presence at multiple levels - State level, district level or local level. This will ensure a secure and containerised operations.

4.2.3 Cloud

The Tamil Nadu State Cloud (Hybrid Model) builds on the State Data Center (SDC) initiative with strong security and privacy policies. This cloud can extend scalable compute, storage, and platform infra services to all future applications across departments. This can host all support systems/ applications/ modules, data and new platforms of several departments of the State. It is also important to consider private cloud from security standpoint and creation of virtual environments from scalability standpoint.

4.2.4 Unique Digital ID

It is important to standardize the process of identification of an individual at any point while providing services. This is the only way to ensure service records created are issued to the actual individual or to obtain consented access through proper consent gateway. Aadhar forms the basis of the national biometric identification system. Government of Tamil Nadu has initiated the 'Makkal Number' which enables a unified database of all citizens. Similar IDs such as PAN, GSTN may be used for businesses. This citizen/business repository will be made available across all departments delivering services. It will also help the Government in better targeting, effective service delivery, greater accountability and efficient monitoring of schemes. It will also help in rolling out a unified payment system to disburse welfare benefits to citizens.

4.2.4.1 Makkal Number

Government of Tamil Nadu has a plan to provide services to the citizens as a predictive service without having to apply for the same. These services include providing government services like certificates, documents, licenses etc. The Tamil Nadu e-governance agency plans to generate a unique ID number for the population of the state called "Makkal Number". The State departments may include and leverage this database while designing their digital transformation strategy.

4.2.5 Service Directories and Registries

Directories play a key role in the service ecosystem as they hold the master data of various entities. Directories must be built with strong ownership and governance mechanism and must adhere to the principle of being the "single source of truth". Directories must be designed to be easily accessible and usable by multiple users, if required anonymously.

4.2.5.1 State Family Database (SFDB)

Government of Tamil Nadu has travelled a long journey to identify the challenges related to beneficiary schemes/ programs such as data discrepancy, inclusion and exclusion errors,

eligibility credentials of applicants, and so on. To address such issues, IT&DS department has initiated the State Family Database (SFDB) that will be aligned to the TNEA. This initiative is envisaged to be a single source of citizen/ resident data for the Government of Tamil Nadu. Further, SFDB will form the core of the Data Exchange Framework conceptualized under the Blockchain Policy.

The database is maintained in a digitized, centralized and secure manner for the purpose of seamless beneficiary identification to disburse benefits provided by different welfare schemes to eligible citizens. Data available with different departments will be de-duplicated and brought into a single database. SFDB would become the foundational database for all citizen / resident information that would be used for Single Sign-On (SSO) and seamless beneficiary identification to disburse benefits / services by different welfare schemes / departments to eligible citizens. Among multiple applications, SFDB would also pave for proactive service delivery like pre-generation of citizen certificates (community, nativity, etc.) and store them and issue whenever requests are received.

State departments can leverage on this database to develop their own mobile applications, dashboards, portals, etc., to aid their policies, projects, programs, and strategy for service delivery. The departments should align their digital transformation strategy towards using the SFDB as a common database to formulate projects and programmes basing on authentic and uniform information across departments.

It is further emphasised that all individual departments should upgrade the database and their IT systems to the common reference standards or data, application and technology architecture. This is critical and should pave way for development of a common database.

Under SFDB more than 50 APIs are being created to create the Peoples ID or 'Makkal number'. The API link also requires to be updated constantly, whenever there is a change / upgrade in their departments' IT systems. Further SFDB works on the principle of subscription service which might lead to errors if the individual department do not update their database based on inputs from another department.

Population Health Registry (PHR)

Population Health Registry (PHR) of Government of Tamil Nadu is a repository of data pertaining to the health of citizens. The registry shall work based on the SFDB and is envisaged to evolve as the central entity to develop health-based applications, standardize data and benefit from data analytics.

A ten-digit unique identification PHR number is created for all citizens (including migrants) to enable interoperability, synthesize multiple sets of data across time horizons and ease operations related to health. The unique identification number also serves as the proxy for the 8 digit 'Makkal Number' of SFDB, National Digital Health Mission ID, and other existing identifiers of health programmes/schemes like Non-Communicable Disease Programme ID. All departments which work closely with health such as school education, Integrated Child

Development Services, Rural development, Tamil Nadu Corporation for Development of Women can be linked via PHR number.

4.2.6 Centre of Excellence for Emerging Technologies (CEET)

IT&DS Department, Government of Tamilnadu (GoTN) has also established a Centre of Excellence for Emerging Technologies (CEET) to solve the problems of governance, nurturing innovation and provide thought leadership by making use of various emerging new technologies, viz., fourth industrial revolution, Artificial Intelligence & Machine Learning, Blockchain, Internet of Things, Drones and Data Analytics.

Some of the cutting-edge projects that have been taken-up under CEET currently, include: –

- **Face Recognition System**: AI based Face Recognition System (FRS) developed for registering attendance. This system has been put in operation in two government schools in Chennai, at the IT&DS department of GoTN and at IIM Trichy.
- **Pest Identification System**: The TNeGA Pest Identification System will help farmers through an app called 'Uzhavan'. This has a reach of over 5-lakh farmers and provides them with pest diagnosis and helps with remedial measures by analyzing the images.
- **Smart Conversation Assistance**: TNeGA has collaborated with Anna University to develop an automated virtual assistant, which can converse in Tamil with people & guide them in obtaining Government services like Nativity Certificates, Income Certificates, Community Certificates using vernacular 'Natural Language Processing' technology.
- **Artificial Intelligence Lab**: An Artificial Intelligence Lab with high computing power along with high-end servers have been planned to be set up at TNeGA. This lab would also be equipped with prototyping capabilities and necessary equipment such as 3-D printers, IP68 grade packaging, PCB integration modules and the necessary licensed software. Technical departments can utilize this common lab to develop their prototypes for deployment.

The departments of GoTN must leverage the above-mentioned capabilities to improve their service delivery to citizens and businesses apart from digitalizing their own business functions and processes. TNeGA will engage in development, use and proliferation of Emerging technologies across all departments through engagement and defining use cases for solutions. This will be through the proposed iTNT hub.

4.2.7 Ontology

Given the diversity of the State and the Nation, there are many different term / units to identify the same. The Ontology in the architecture provides a service of mapping between different terms, providing a scaling factor where appropriate. To develop and implement standards for common understanding and semantic exchange of information, it is important to develop the ontologies for Government. To begin with, several catalogs are being developed – Electronic service delivery, demographic and administrative data across departments.

4.2.8 Data Analytics

With the availability of different data sets in the database, various data analytics is possible which could benefit the citizens. This will be done through decision support to the stakeholders on a wide variety of themes through analysis of the aggregated datasets. The design must ensure that analytics of data is done on the credible database. The Analytics engine will provide a collection of statistical and Machine learning (ML)/AI algorithms to analysis the historical data and prediction into the future.

4.2.8.1 Tamil Nadu Decision Support System (DeTN)

DeTN is a connected data eco-system that would aid Government in decision making for effective implementation of policy response. This system would establish necessary framework and create infrastructure for supporting and maintaining open data sharing, warehousing and tools to connect diverse datasets. This system will have domain driven, purpose driven and function driven dashboards. This document will help departments in digitalizing their operations and providing granular and real-time data for data driven decision and policy making.

CM Dashboard is a real time monitoring and interactive dashboard for the Chief Minister. It shall include all major schemes, projects of individual line departments at the strategic level to help decision making and proactive interventions required which uses first level data. The departmental dashboard on the other hand will have access to real time granular data of the projects and schemes, including individual beneficiaries and benefits availed by them. It will provide data driven insights to departments to improve efficiency and policy making. It shall also be linked to the Grievance redressal portal and it should be possible to drill down to obtain details pertaining to details of any individual.

4.2.9 State Information Exchange Platform (SIEP)

All actors in the service delivery ecosystem would in some way or other be generating or accessing various services information, using one or more access applications. The exchange of information needs to be enabled as real-time data exchange by implementing Open APIs with role-based access control. Each access application to submit, retrieve or access any information, must be registered with the State Information Exchange platform (SIEP). The SIEP would be responsible for authentication and authorization of all data exchange requests. The requesting entity, including application, official, citizen, business, etc., would provide credentials appropriate to its role and act as permissioned.

4.2.10 GIS Visualization

Geographical Information System (GIS) Visualization services can be used to enable effective localized decision making. Capture and use of spatial dimension should be mandated across the entire data life cycle and collection through analytics and visualization. This will support answers to various queries such as finding the nearest service center with a required facility or plotting of service demand in a geographic area. The GIS services will also help in

State/district/local level planning and monitoring of various digital services offered by the serving departments.

4.2.10.1 Tamil Nadu Geographic Information System (TNGIS)

In Tamil Nadu, vast spatial data has been generated through GIS projects undertaken by various state departments. The basic challenge has been to put the huge volume of existing data sets in decision making process. Different agencies are developing GIS on different platforms leading to inability to scale up, being, spatial / locational inaccuracy of information, mismatch in data, lack of update of data over time and use of non-standard tools (proprietary versus open-source software tools) in managing the data sets.

To address these issues, Tamil Nadu Geographic Information System (TNGIS) has been conceived to create a generic model of GIS and to easily integrate with other available data sets. This will provide a uniform GIS platform over the state. This helps in taking necessary decisions in various state departments as well as providing services to the citizens. It is proposed to establish a digital maps repository which would serve these purposes. The departments while drafting their digital transformation strategy can align their digital transformation projects/ programmes/ initiatives to use TNGIS data.

4.2.11 Improved Service Delivery

Electronic service delivery initiatives should ease the life of the common citizen and improve efficiency and effectiveness of Governance and administration. In most of the cases, the departments have computerized the existing physical process only. Governance process re-engineering (GPR) shall be undertaken to reduce the unnecessary procedures and processes involved in issue of permit/permissions/services to improve ease of doing business and citizen experience. The Service Delivery framework should focus on the following elements:

- ***Accessibility***: Accessibility is a necessary element for good transactional user experiences, including two-way communication. In the case of Government web-sites, these experiences can include enabling users to create personal login on the portal, availability of SSO feature for users to sign-in through an integrated authentication initiative and availability of installable mobile applications for providing information and services. Accessibility allows people with a diverse range of hearing, movement, sight, cognitive, linguistic, and technological abilities to equally access, understand and navigate through a portal and its services without any restrictions.
- ***Content Availability***: The ability to understand and use the content on Government portals determines the extent to which people can participate in the economy through electronic media. Therefore, the definition embeds five key dimensions – quality, presentation, understandability, local language and ease of sharing. It shall be ensured that availability of updated, authentic, relevant, and user-friendly information in Tamil, which can be easily understood and shared through multiple sources such as email and social media.
- ***Ease of Use***: It encompasses different aspects like system usability, flexibility, system control, user adaptability to the system. This is a critical factor on which the adoption and satisfaction of e-Government services by users depends. It significantly influences

user satisfaction, their perception regarding benefits of the system and subsequently their intention to use the system. It is the degree to which a user believes that usage of a system shall be free from effort or difficulty. It includes easy content exploration, findability, task efficiency and automation.

- ***Information Security***: Safety and integrity of information shared by the citizen with the Government for any digital transactions should be of utmost priority. This can be ensured through secured networks, robust applications, data privacy policies and frameworks and security operations centers.
- ***End Service Delivery*** includes consideration of parameters such as:
    - ✓ Ensure that all digital services and corresponding electronic records are in accordance with Tamil Nadu Information Technology (Electronic Service Delivery) Rules, 2016;
    - ✓ Ensure that the service delivery timelines are published on the website;
    - ✓ Ensure that the manual processes have been completely prohibited in service delivery; and
    - ✓ End Service Delivery measures the citizens' satisfaction with faster delivery of end services, elimination of manual processes, reduction of time/ manual effort to obtain a particular service.
- ***Integrated Service Delivery***: The term "integrated service" consists of two parts: service and integration. In e-Government parlance, 'service or e-service' is a set of activities delivered by Government agencies that is facilitated by information technology. Providing effective and efficient e-services requires the integration of e-services across all levels and branches of Government agencies collaborating with each other. This enables seamless service delivery when multiple departments are involved in service processing and demonstrates the 'whole of government' approach to users.
- ***Status and Request Tracking***: For every service request submitted by citizen, either, manually or online, a unique service request or application number should be issued to the citizen. This shall be standardized across all departments. In reference to this unique number, the status of the request can be tracked by the citizen through various channels such as website, SMS, call-center, emails. Further, the Government agency should proactively communicate the status to the citizens through the choice of channel opted by the citizen. A mechanism through which the citizen can get to know the stage at which his / her service request is at using the unique Service Request Number or Application Number.
- ***Feedback mechanisms***: For all services and functions of state departments, it is critical to include a robust mechanism in place for collecting and processing the feedback from the public/users for continuous improvements. The Biz Buddy platform developed in Guidance based on specific officer-based timelines has been very successful in bringing different digital maturity departments into a common grievance redressal framework[2]. A cross-departmental statewide SLA based system can be integrated into Integrated and Inclusive Public Grievance CM Helpline Management System (IIPGCMS).

[2] Towards Real-Time Governance: Using Digital Feedback to Improve Service, Voice, and Accountability https://www.cgdev.org/sites/default/files/towards-real-time-governance-using-digital-feedback-improve-service-voice.pdf

4.2.11.1 Nambikkai Inaiyam (Blockchain Backbone)

GoTN released the Tamil Nadu Blockchain Policy 2020 to institutionalize the use of Blockchain technology for betterment of services and functions in the state departments. The Tamil Nadu Blockchain Policy 2020 recommends providing a semi-regulated sandbox environment for building e-governance applications using Blockchain. Application developers for the Blockchain backbone need access to a controlled testing environment for building and testing products and services. This controlled environment needs to be a complete or partial replica of the live environment with slightly relaxed regulations, so developers can recreate real time scenarios and observe the behavior of the applications and test the project's viability. Blockchain has proven applications in sectors like healthcare, tax filing, voting, bank transactions, land registry and identity management. Any state department can make use of the technology to serve its unique challenges.

Blockchain technology has many benefits to government departments because of the technology's reliability, mechanisms available for transparency, immutability, and its ability to save intermediary and operational costs. In lieu of Tamil Nadu Blockchain Policy, the blockchain backbone was initiated by IT&DS Dept, GoTN. This initiative can be leveraged by the state departments for reimagining governance and for encouraging the adoption of Blockchain. Some of the use cases of Blockchain technology are listed in the box below.

Use cases of blockchain

- **Forest** - For securing and verifying tree felling and transit licenses and sawmill licenses, certifying and tracking Orthodox Nilgiris Tea, ivory products and red sanders and sandalwood products and tracking captive elephants using blockchain.
- **PWD** - For creating asset registry and monitor/ predict the several aspects of each asset such as age of the assets, revenue generated, expenditure patters of assets.
- **School education, Higher education** - For securing education certificates, marksheets, degrees, diplomas.
- **Revenue Administration Department** – For Income Certificates, Community Certificates, Caste Certificates, Nativity Certificates, Birth certificates, Death certificates, Drug License and other licenses for citizens and businesses/ Generating, securing, and verifying certificates, documents and licenses.
- **Handlooms, Handicrafts, Textiles and Khadi Department** - For certifying handicrafts and handlooms made in Tamil Nadu and identifying counterfeits
- Website, data and document integrity for government organizations, departments and agencies, public sector enterprises and others

4.2.11.2 Predictive Services Initiative

IT&DS dept., has envisioned to develop technology architecture and platform to enable proactive and seamless delivery of government services to targeted beneficiaries and availing citizens. Predictive Services architecture consist of the following major software components:

- *Data Exchange Framework;*
- *Event Driven Services Engine;*
- *Service Management Platform;*
- *Identity & Consent Management; and*
- *User Portals, Dashboard & Analytics.*

The above components will be built on top of the software interfaces and databases developed as part of SFDB and Blockchain initiatives. Benefits of this to various departments include improving efficiency, effectiveness and transparency of services delivered.

As discussed, the departments while drafting their digital transformation strategy should leverage on the predictive data analytics and architecture to improve their service delivery to citizens and businesses apart from their own functions. The techniques and tools of data science can be proactively used and citizen centric governance can be delivered in an integrated approach.

4.2.11.3 E-Sevai 2.0

Under e-Sevai 2.0, Department of IT&DS has envisaged the next generation single platform for all citizen centric services integrating all standalone services of various government departments. Government departments, while designing and implementing their digital transformation strategy can then launch services online in a quick and easy way allowing for streamlining of their processes, connecting all the stakeholders and improve the delivery efficiency of their services.

The Tamil Nadu Integrated Services Platform would have the core features such as:

- Every service should be available and accessible online in Tamil and English – eSevai centers, citizen web App and Mobile App (Makkal Sevai), Chatbot (web and mobile), Voice bot on mobile (wherever possible), doorstep delivery (wherever feasible) etc. Each service developed would be deployed in multiple channels and modes simultaneously.
- A unique application ID will be generated irrespective of channel and mode and citizens must be informed of the status at each stage of the service delivery.
- Core Platform will enable line departments to deploy highly automated applications with minimal development to meet evolving policy needs and real-time governance requirements.
- The platform would have an independent module that allows managing the activities of eSevai operators, evaluate their performance, allows onboarding of third-party services to be delivered by the operators and allows tracking of all services offered through a single portal.
- A two-way multi-channel (online chat, SMS, email, WhatsApp) communication and interactivity will be provided between citizens and officers through the Customer Relationship Management features.
- All the interactions shall be recorded.

- Online office hours can be setup for district collectors and other senior officers for seeking clarifications.
- The platform will allow creation of end-to-end G2C services with interim G2G process steps abstracted and published as independent web application. Thus, this platform will allow building physical to digital and integrating existing digital to single platform.
- Data encryption, masking, anonymization should be implemented though the data life cycle to protect the personal data.
- Implement an integrated platform, applications, data and services architecture to bring all the citizen services on the same platform.
- Configurable and shareable reports and dashboards based on roles and privileges.
- The platform will be integrated with APIs open for each service as if it were to be initiated though external platforms (like making community certificate service available over Umang App). The shareable APIs should be published on API Setup or similar platform so the department applications wanting to launch service from their portals or embed the process step in internal workflows should be able to do so using the published APIs.
- Core Platform will enable development of common applications like performance management, productivity tools, workflow management, core data management, messaging, notification, user management, system administration and security.
- The common applications will be built centrally and used in common by all line departments, with appropriate configuration required by each department.
- AI enabled Voice bot, chatbots for getting information and availing services.
- AI enabled Document management system for easy processing of services (OCR/ field validation).
- Citizens should be able to raise a grievance on the application submitted from the same portal/mobile app. The grievances could also be registered using other methods like calling helpline or WhatsApp or email.

Government is working with the vision to deliver all services online to Citizens even in the remotest corner of the State through Arasu eSevai Centres. Services provided by different government departments must transition to the common platform.

4.2.11.4 Know Your Government

IT &DS dept., is developing a web and mobile application platform called “Know Your Government” to provide services of accessing the government facilities on a GIS enabled Map, in which, the public can search and access any government facilities such as Police Stations, Health Care Facilities, Govt. Schools in their proximity. The departments, while drafting their digital transformation strategy may take advantage of this web and mobile application for better public reach.

4.2.11.5 Single Window System

Guidance is the Nodal Agency for improving the 'Ease of Doing Business' in the State of Tamil Nadu and has developed the Single Window Portal (SWP) which will act as a single point for accepting and electronically distributing applications regarding services provided to enterprises by the departments in the State of Tamil Nadu. This has been developed with the objective of improving the business climate of Tamil Nadu. The departments while drafting their G2B digital transformation strategy can leverage SWP to improve their service delivery to businesses.

4.2.11.6 E-Office

E-Office initiative is aimed towards conducting office procedures electronically. The objective of implementing e-Office is to eliminate the use of paper and to make most of the office communication electronic. The following are advantages of this initiative:

- To improve efficiency, consistency and effectiveness of Government responses;
- To reduce turnaround time and to meet the demands of the citizen charter;
- To provide for effective resource management to improve the quality of administration;
- To establish transparency and accountability;
- To provide a cost-effective e-Storage facility; and
- Eco-friendly government ecosystem.

The e-Office would enable the electronic file management system for speedy disposals of files, resulting in better utilization of manpower, thereby avoiding delays, leading to better governance. It will be rolled out in the entire State by 2023.

4.2.11.7 IIPGCMS

GoTN's IIPGCMS aims to streamline addressing citizen grievances by bringing them onto a single platform. This platform captures the complaints and grievances received through various channels across digital and non-digital modes. Complaints registered by citizens on social media, through call centers, petitions, and so on, are brought on to a single platform, from where nodal officers across different departments are notified towards addressing them. Citizens are updated about the status of their complaint and advised about further possible actions that could be taken, as per their judgement. IIPGCMS (CM Helpline) is an inclusive, integrated, and convenient public grievance redressal platform, where citizens can:

- File and track grievances related to government services, schemes, and civic issues;
- File grievance via multiple channels – calling the helpline, web portal, mobile app, e-mail, Twitter, Facebook, by post or by visiting the grievance call center in person; and
- Ask questions, provide suggestions and see announcements from the CM.

Grievance workflow in IIPGCMS:

- Grievance is registered digitally;

- Grievance mapped to grievance ID to help the public track progress;
- Officers from respective departments accept/reject/assign and redirect grievances; and
- Publicly available Dashboard to track progress of grievances.

CM Helpline Call Center facility in Sholinganallur is operational and scalable at a short notice. The departments while drafting their digital transformation strategy must include considering redefining their procedures and systems and align them to the IIPGCMS for feedback and grievance mechanism for their services and functions.

4.2.11.8 Citizen Centric Digital Interventions

The Citizen will be the center focus of any digital intervention in the State. Digital transformation should be initiated only after a detailed understanding of the needs of the citizen. A dashboard shall be made available to every citizen of the State who is interested in knowing the schemes/services. One should be able to apply for any service of any Government department. The citizen can use the same portal to know about the status of the application, a repository to download the documents related to their interaction with citizen. The same portal should act as a Grievance redressal channel as well. All the services of various departments shall be integrated with this dashboard. The ultimate objective of this dashboard will be to act as a one-stop shop for every interaction between the Citizen and the Government.

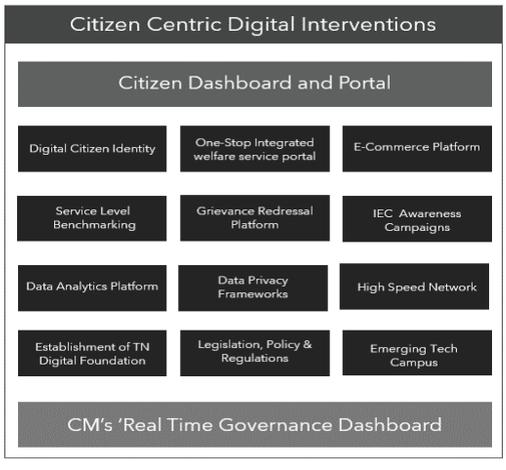
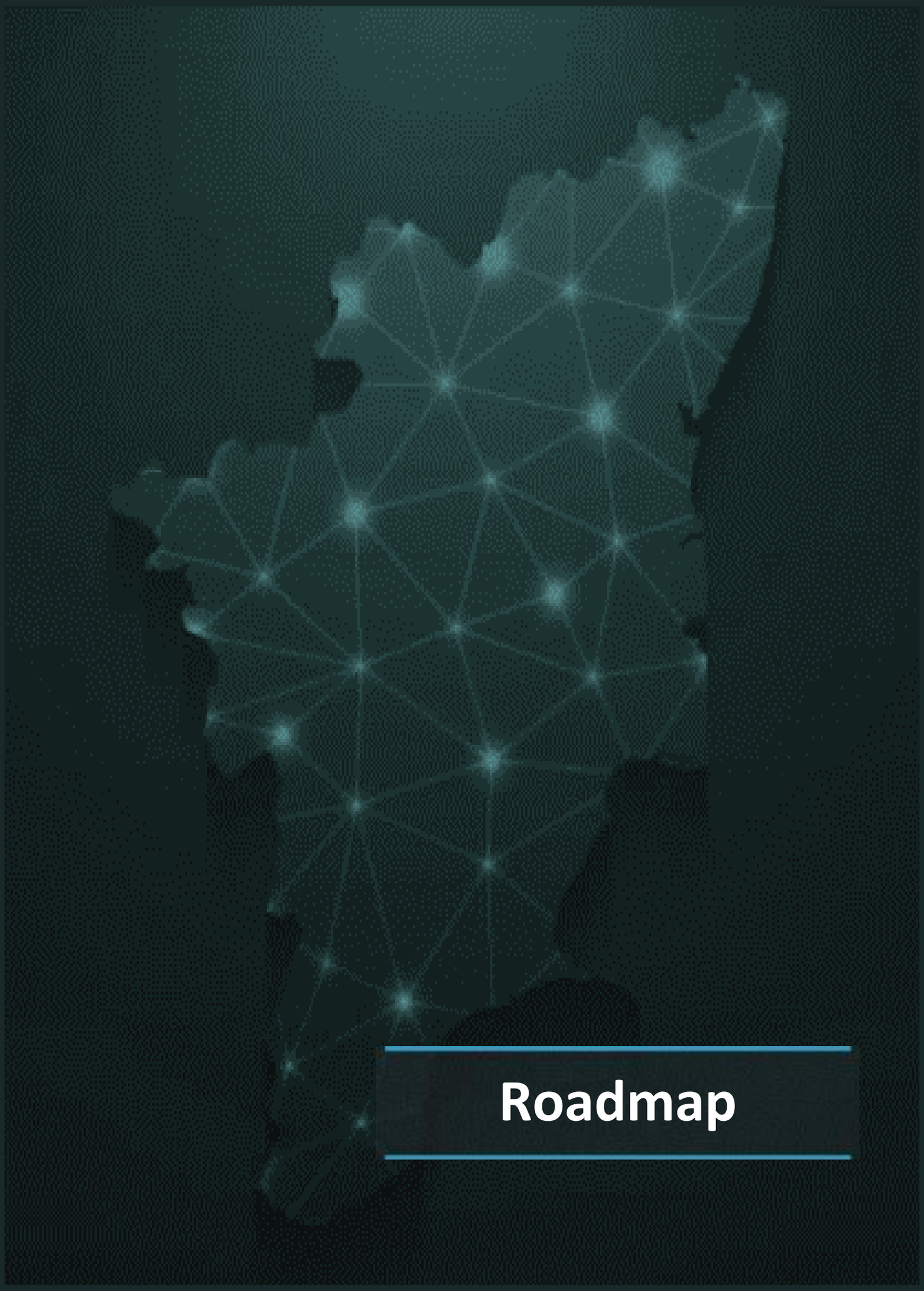


Figure 6: Citizen centric digital interventions

4.2.12 Planned State level Digital initiatives

The GoTN is taking steps to provide an integrated portal for all the services rendered along with a digital locker to store and retrieve their records/data. There shall be adequate Information, Education and Communication (IEC) campaigns in the local language to enhance digital literacy and awareness quotient. Grievance redressal mechanisms, data privacy frameworks and change management initiatives shall conform to citizen-centric and citizen-driven governance approaches for all transformations planned.



Roadmap

5 Digital Transformation Implementation Roadmap

The success of DiTN lies in adopting an implementation strategy that can produce tangible results in a time bound and phased manner. Hence, a four-pronged approach with focus on early harvest programs, streamlining data and applications, extending required IT support to departments in all stages, creation, and deployment of a dedicated IT team to help departments from existing vacant posts by IT&DS dept, formulating necessary policies and standards in line with process and technology changes adopted in transforming the service has been adopted.

Figure 7: Implementation Approach

5.1 Implementation Strategy

Implementation strategy aims at total digital transformation of the services while increasing shared solutions /multi-functional services as envisaged in the State Level IT Architecture. It also aims to achieve full utilization of existing infrastructure and planned expansion with scalable designs, as listed in section 4.2. All applications, APIs and data structures developed shall conform to interoperability framework. The implementation strategy involves a multi-step process of digital maturity assessment, project selection, service categorization & portfolio construction and finally prioritization. The execution would be carried out in multiple phases with each phase delivering tangible value to citizens.

5.1.1 Digital Maturity Assessment

It is important to group the departments based on their level of digital maturity/ digital readiness, and accordingly define their implementation timelines for full digital transformation. The departments may consider using the below mentioned self-evaluation framework to assess their digital readiness and categorize into: (a) Urgent, (b) Most important, and (c) Important.

Table 2: Self-Evaluation framework for department's digital readiness/ maturity (Illustrative)

#	Parameters	Factors (Indicative)	Urgent	Most Important	Important
1.	Performance	% of services with KPIs; % of KPIs linked to incentives to employees; % of KPIs with digital tracking mechanisms, etc.	<50%	50-70%	>70%
2.	Business	% of business processes digitized; % of files managed in e-Office for internal and external, etc.	<50%	50-70%	>70%
3.	Integration	% of systems interfacing with each other within the department; % of systems interfacing with other departments, etc.	<50%	50-70%	>70%
4.	Application	% of services online (as required)	<50%	50-70%	>70%
5.	Data	% reliance on open source; % adoption of open standards; Are the systems/	<50%	50-70%	>70%

		applications cloud compatibility; % adoption of emerging and disruptive technologies; etc.			
6.	Technology	% open standards used for applications/ systems; % shared infrastructure used for hosting applications/ systems; % Micro Services used in applications; etc.	<50%	50 70%	>70%
7.	Security	Availability of data Integrity strategy, Data Privacy & Confidentiality, regular threat vulnerability assessments, etc.	No	Partial	Yes
8.	Governance	Availability of governance structure and teams to design, develop and implement digital transformation strategy	No	Partial	Yes

The departments must carry out a self-assessment of their digital readiness and state their targeted digital readiness and accordingly draft their programs/ initiatives/ projects to achieve the proposed digital transformation ecosystem. A detailed self-assessment report of department's current state of digital readiness is the first step in formulating their digital transformation strategy.

5.1.2 Project Identification & Selection

Based on the digital maturity assessment, departments can carve out the projects across the key focus areas listed in section to realize the vision. Departments can take 'outside-in' approach to see what possibilities exist to improve on 'connected citizen', 'promoting digital economy' and 'transformed service delivery'. This will be based on the emergence of new technologies, change in legal/regulatory environment and changes in socio-cultural preferences. Similarly, departments can also take an 'inside-out' approach to identify opportunities to realize the vision based on existing technical systems, digital maturity, new capabilities added within the department, new responsibilities assigned and as mandated by the Government.

5.1.3 Services Categorization and Portfolio construction

Initiatives/ programs/ projects in Digital Transformation strategy can also consider types of services offered by department – *G2C, G2B and G2G*.

1. **G2C Services**: This is crucial as it impacts the citizens directly. An example of initiative which can be prioritized could be pertaining to the healthcare sector. A comprehensive health management system – at primary, secondary and tertiary health care facilities operated by the government which can be utilized to streamline the process of delivering healthcare services would improve overall quality of life, satisfaction, and aid in saving the costs.
2. **G2B Services**: Services targeting businesses are of key significance as they help in the overall economic development of the State. An example of initiative in this category could be the implementation of a digital solution to help with investment promotion and incentive scheme aimed at Micro, Small and Medium Industries in the state.
3. **G2G Services**: The government and its departments are one of the leading employment generators. Given that it impacts millions of employees, focusing on

services pertaining to them can also have a significant efficiency multiplier in functioning of the government machinery which in turn can have multiplier effect on other types of services. An example of this initiative is e-office solution and HRMS, Asset Management System to streamline file movement and employee processes and assets across departments.

The approach for this can be classified into three categories depending upon the timeline for implementation as follows:

A. **Category-A** digital initiatives / projects / programs
    a. Timeframe: 6 to 12 months;
    b. Departments / services having widespread impact or requiring immediate and urgent interventions; and
    c. Projects / initiatives which require less effort / budget to reach to desired objective.
B. **Category-B** digital initiatives/ projects/ programs
    a. Timeframe: 12 to 24 months;
    b. Departments / services having low-medium level of digital readiness or requirement most important interventions; and
    c. Services having complex integration between departments for implementation.
C. **Category-C** digital initiatives / projects / programs
    a. Timeframe: 24 to 36 months;
    b. Departments / services having zero level of digital readiness; and
    c. Limited technology interventions available currently and that requires R&D.

Also, the roadmap for digital transformation and action plan shall be based on short, medium, and long-term priorities based on strategic shortlisting of departmental initiatives via various parameters viz.,

- ✓ Citizen-centricity;
- ✓ High volume transactions;
- ✓ High Impact;
- ✓ Strategic (indicates importance considering manifesto or Govt policies) ; and
- ✓ Priority (indicates only start date of the transformation initiatives and not ranking)

5.1.4 Project/Portfolio prioritization

The prioritization and selection of target service portfolio will be done by the respective departments for which necessary budget provision will be provided to departments to execute e-governance projects to achieve the objectives of DiTN strategy . This approach will lead to increased buy-in from the departments and will greatly improve the probability

of success for the digital transformation initiatives and easier to achieve all milestones planned. Some of the indicative criteria for shortlisting of projects from the pool of projects could be:

- ✓ Potential impact in terms of service delivery efficiency, social and economic benefits;
- ✓ Usage of emerging technologies in overall optimization;
- ✓ Estimated cost savings;
- ✓ Process excellence in digital transformation;
- ✓ Universalizing access of services to the citizens and businesses (incl. various e-services);
- ✓ Utilization of local resources; and
- ✓ Innovativeness in the approach.

5.1.5 Execution of the strategy

Based on the maturity level of each department, department level digital transformation strategy can include an implementation roadmap for all the inventory of digital projects / programs / initiatives that are identified. This roadmap for each department will be executed in phased manner in consultation with IT&DS department. It is important to identify those transformation initiatives / projects/ programs which can be implemented in shorter span of time and provide greater impact and get closer to the overall department digital transformation strategy and state level digital transformation vision and focus areas.

5.2 Digital Transformation Governance Framework

The successful achievement of the Digital Transformation Policy will depend on an integrated approach during implementation supported by developing strategic synergies and partnerships. This implies that clear definition of the roles, responsibilities and functions of all stakeholders must be made.

The Digital Transformation envisages three-tier Governance framework to successfully deliver the across various sectors / departments in the State. The graphical representation below explains the TNEA Governance Framework:

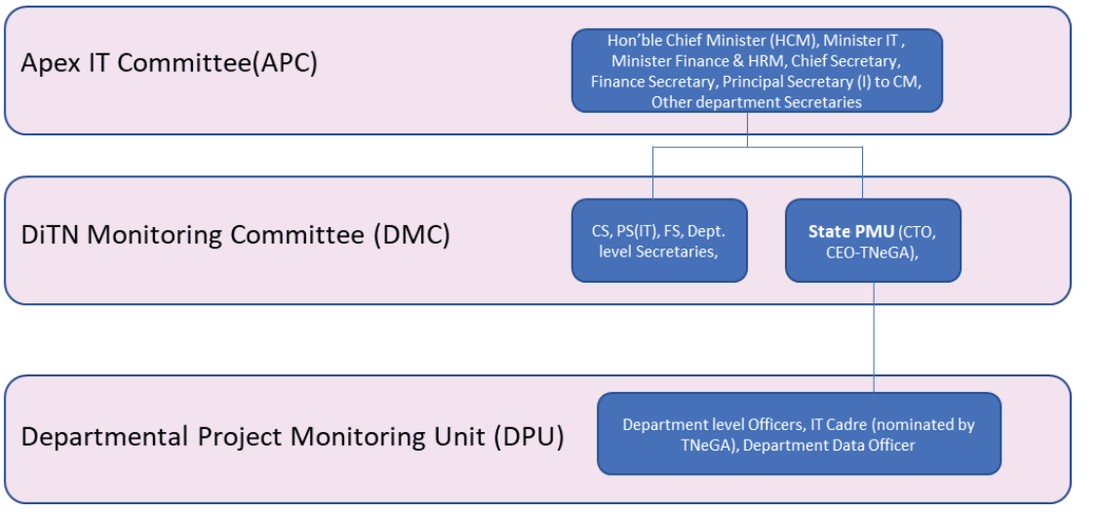


Figure 8: Digital Transformation Governance Framework

The roles and responsibilities of key stakeholders of **Digital Transformation Governance Framework** are described in the following sections.

5.2.1 Apex IT Committee (APC)

a. The Apex IT committee (APC) would provide strategic guidance to the overall State digitalization program. APC will provide for policy and monitoring, guidance, leadership, prescribe deliverables and milestones. It will evaluate periodically and direct the DiTN Monitoring Committee (DMC) to take remedial actions if any.

The Apex IT committee shall be chaired by the Hon'ble Chief Minister, with Minister IT&DS Minister Finance & HRM, Chief Secretary, Finance Secretary, Principal Secretary (I) to Hon'ble Chief Minister as members. Other departmental secretaries whose projects are being reviewed shall be invitees. Secretary (IT&DS) shall be the member secretary of APC.

The **key roles and responsibilities** of APC include:

- Provide visionary and catalysing leadership at the highest level of Government to Support the implementation of the Policy
- Provide guidance and direction to all departments in execution of its mandate;
- Set the IT vision for the state; and
- Provide Strategic guidance to DMC.

5.2.2 DiTN Monitoring Committee (DMC)

The DMC would drive the state-wide implementation of DiTN. It shall review and monitor the progress of Digital Tamil Nadu implementation based on APC decisions. It shall be chaired by the Chief Secretary with Secretary IT&DS as its Member Secretary. Finance Secretary, Secretaries of the respective departments who are digitalizing their operations will be members, along with Chief Technology Officer (CTO) of IT&DS department and the CEO TNeGA, and members of the State Project Monitoring Unit (SPMU).

All e-Gov projects of all departments shall be brought to the committee for monitoring, guidance, review, and recommendation. It shall also pursue with departments to take up relevant e-Gov projects which are the priority of the Government. However, for approval of e-Gov/IT projects, the existing process of approval and circulation through IT&DS Department and Finance be followed. It shall also ensure resolution of project difficulties including inter-departmental issues during project execution.

It shall, as required, review all major IT projects being implemented in the state to ensure an integrated approach. This committee would drive the architecture design and rollout for select sector / departments along with the departmental stakeholders. Its main role will be to ensure synergy among various e-governance / IT initiatives proposed for or by the respective state departments and ensure uniformity of design and standards across departments.

The **key roles and responsibilities** of DMC include:

- Integrate the structural requirements of DiTN across all departments;
- Improve selection and use of new technologies for implementation of the policy;

- Synergise and rationalize DiTN Implementation across all departments;
- Setup of Digital transformation across the State; (Architecture, Infrastructure, Application, etc.)
- Approve policy/orders/instructions relating to implementation of DiTN;
- Review e-gov / hardware procurement progress of all departments.
- Coordinate across all state departments for e-governance/ IT initiatives;
- Oversee implementation activities.
- Resolve conflicts arising out of implementation related activities.
- Review and issue instructions on departmental digitalization initiatives which are functioning without any integration with other systems.
- Ensuring that good governance principles are applied and adhered to in the implementation of the Policy ;

5.2.3 State Project Management Unit (SPMU)

TNeGA will function as the state level Project Management Unit (SPMU) to provide functional, technical, and managerial inputs to the DMC. The Chief Technology Officer (CTO) of IT &DS department will oversee all IT projects being implemented through TNeGA.

The **Key roles and responsibilities** include:

- To provide support to all departments to steer and anchor the policy implementation initiatives;
- To support the DMC in all its initiatives with policy and implementation related issues and new initiatives necessitated;
- To support departments in crafting progressive e-Governance strategies, to promote SMART- Swift, Monitorable, Accessible, Responsive, and Transparent Governance;
- To promote innovation and evolve models for empowerment of citizens through the policy initiatives and to promote participatory governance ;
- To develop a statistical strategy for measuring the goals of this policy and also to create appropriate data sources;
- To put in place an institutional mechanism for capacity building of all department and its agencies, including assessment and evolution of suitable training packages/modules for capacity building to enhance competitiveness for successful implementation of the policy including to cut on cost and time over run;
- Coordinate with all the state departments to identify the vision/ mission statements, their short, medium, and long-term e-governance and IT initiatives/plans;
- Perform and support necessary support-related activities under DiTN implementation of the architecture for all departments and agencies;
- Support on maintenance of IT infrastructure assets in departments, functioning with hi-tech labs;
- Provide technical assistance in designing e-governance/ IT initiatives across state departments/ agencies;

- Provide project implementation support to state departments/ agencies during development and implementation of e-governance/ IT initiatives;
- Facilitate design and rollout of SSO mechanism for all departments; and
- Communicate and share Information amongst stakeholders for efficient implementation;
- Implement the directions of DMC; and
- Submit periodic status reports to DMC on the progress of implementation of e-governance/ IT initiatives at state departments/ agencies.

5.2.4 Departmental Project Monitoring Unit (DPU)

Each department executing an e-Government program / IT initiative will have a dedicated Departmental Project Monitoring Unit (DPU). The DPU will comprise of the Officer responsible for the project in the department; functional technical / IT consultants available in the department; the IT cadre resources (nominated by TNeGA); and the designated Data officer of the department. The DPUs shall administratively be controlled and report to SPMU

The inhouse team at department level shall be responsible for the department's digital initiatives / interface for the rollout of DiTN. Whenever additional skillsets are required for the department, the same will be made available by TNeGA/ELCOT. Considering the fast-paced development of IT and technology applications, a healthy mix of outsourced, contract, and timescale employees shall be maintained.

The **Key roles and responsibilities will** include:

- Coordinate with SPMU for technical, functional, financial requirements for designing, developing, and implementing department level e-governance / IT initiatives ;
- Prepare department level digital governance / transformation strategy ;
- Draft vision, mission, and objectives of the department in improving service delivery;
- Consolidate and analyze the list of services offered by the department;
- Consolidate and analyze the list of IT applications / systems currently used by the department for the service delivery;
- Support each department to have single portal pertinent to schemes, progress, and project management. Conduct feedback surveys to understand the issues faced by the citizens and businesses and their requirements to improve service delivery;
- Develop implementation plan and cost estimates for the proposed recommendations;
- Preparation of Tender documents and carrying out bid process management to bring the system integrator/ consultants on board to develop the proposed systems and policies;
- Periodic evaluations of the projects / programs and take-up corrective measures during the implementation; and

- Conduct mid-term and End-term project/ program evaluations to report the achievements and lessons.

5.3 Capacity Building and Change Management

GoTN intends to invest in change management practices across various levels to build capacity and skills, develop human resources, improve digital literacy (e.g., Role mapping in terms of what we have and what we need to implement Digital transformation), and promote digital platforms. Changing the culture and behaviors of an organization is an organic process, not an engineering one, and one that will take time. The working culture shall have inclusive strategy of bottom-up approach for participation of all stakeholders.

The change management team will be a part of the PMU and will drive culture changes by creating tools, policies and governance models that encourage innovation, challenge, agile development, data driven decision making approach, openness, flexibility, and service orientation. It will encourage a multi-pronged approach to address domain and technology skill gaps at policy, program, and project level levels through:

- ✓ Conducting continuous and customized capacity building programs by in-house programs and external trainings throughout the career of government and public sector employees. Reviewing staffing requirements, integrate digital capability, process, and prioritize recruitment at each unit or department delivering digital functions. Encouraging internships, fellowship programs, crowdsourcing, hiring for short-term assignment, outsourcing models to address lack of adequate skilled workforce;
- ✓ Computer Concepts Certificate (CCC) exam in a timebound manner shall be made compulsory for all the current employees from entry position to senior level;
- ✓ Periodic trainings on digital competency / literacy shall be conducted to enhance and upgrade on digital skills;
- ✓ Offering courses that will be designed and made available to the staff to read and understand both in online and offline mode. Periodic examinations shall be encouraged to be conducted on the courses in online mode. A pass in these examinations with minimum percentage of marks could be one of the factors in considering promotions to next higher level and salary increments;
- ✓ In addition, staffs shall undergo mandatory orientation programme along with other departmental exams as a part of periodical upskilling;
- ✓ Facilitating industry exposure on technology and business domains to ICT staff supporting the digital ecosystem;
- ✓ Collaborate with educational institutions (schools / colleges / universities) to promote digital skillsets and for suitable addition in curriculum;
- ✓ Sustained awareness campaigns and regular public outreach programs;

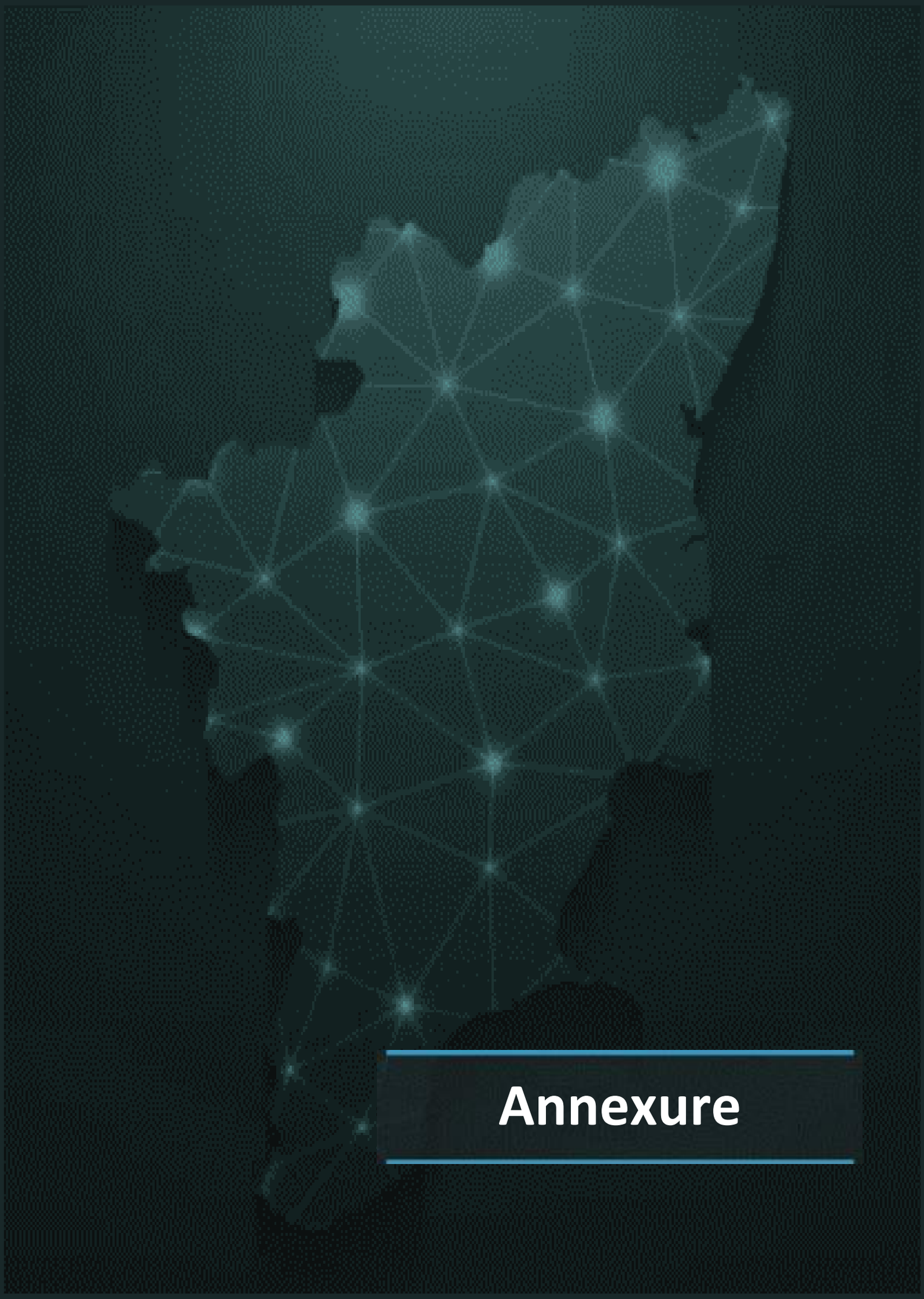
- ✓ Work From Home and Work from Anywhere may be an added options for staffs of certain departments with appropriate supervisory mechanism in place;
- ✓ The Inhouse IT team attached with the department with technical expertise shall be equipped to resolve IT issues and provide handholding to non-technical IT staffs;
- ✓ Each staff within the department shall be trained with cyber security knowledge, managed by Chief Information Security Officer (CISO) through various information security programmes;
- ✓ Basic knowledge of computer applications will be required for all recruitments including for ministerial staff in the cadre of Junior Assistants/Assistants/Typists; and
- ✓ All officials must be trained and retrained in computer applications and new technology every 5 years.

5.4 Way Forward

As the way forward, each department identified for digital transformation should undertake a detailed study and prepare an improvement strategy and roadmap for digital transformation. Some of the activities to be undertaken include:

- ✓ Stakeholder interactions and workshops to understand department's vision, objectives, roles & responsibilities, functions, services, and key priorities;
- ✓ Identifying and cataloguing the G2G, G2B and G2C services of the department;
- ✓ Identify the current service KPIs, challenges, bottlenecks, performance management systems and standards;
- ✓ Conducting voice of customer survey to identify the key challenges in service delivery from the departments, analyze the feedback and identify key issues that needs priority in resolution; and
- ✓ Defining interventions and priorities for implementation, with focus on automation and modernization through IT enablement, for addressing the challenges in current service delivery framework.

For detailed scope of activities, refer annexure. These activities will be enabled by Department of IT&DS through TNeGA



Annexure

6 Annexure

6.1 Scope of work/ list of activities

This section discusses the list of activities/ scope to be carried out by each department to **design, develop and implement the department specific digital transformation strategy/ plans**. This section clearly articulates the list of activities to be carried out by each department to implement the recommendations derived from This section covers the entire lifecycle of implementing department's digital transformation strategy.

Table 3: Overall scope

Scope	Coverage
Design and Implementation Requirements	*a. Design digital transformation strategy* *b. Design and Implementation (incl. development) of Application/ Software derived from digital transformation strategy* *c. Implementation of IT infrastructure to support the applications/ software* *d. Training, Capacity building and Change management Services* *e. Data Digitization and Migration*
Support Services Requirements	*a. Establishment and management of Helpdesk Operations* *b. Warranty and Maintenance Support of Application and System Software* *c. Warranty, Operations and Maintenance Support for IT Infrastructure*

a. Design digital transformation strategy/ plans

The table below presents the list of activities for designing digital transformation strategy/ plans.

Table 4: List of activities for Designing Digital Transformation Strategy/ Plans

Scope/ Timelines	Detailed list of activities
Design digital transformation strategy/ plans **(3-6 months)**	Develop a comprehensive digital transformation strategy containing sufficient details on department's vision statements, goals, and timelines for every activity for implementation. The digital transformation plan should capture - • Draft vision, mission, and objectives of the department in improving their service delivery

Scope/ Timelines	Detailed list of activities
	• Consolidate and analyze the list of G2G, G2B and G2C services offered by the department • Consolidate and analyze the list of IT applications/ systems currently used by the department for the service delivery • Identify the key issues and challenges faced by the department during service delivery • Conduct feedback surveys to understand the issues faced by the citizens and businesses and their requirements to improve the service delivery • Draft department's envisaged interventions/ solutions to address the identified issues/challenges • Develop implementation plan and cost estimates for the proposed recommendations

b. Design and implement proposed recommendations/ IT solutions/ applications, derived from Digital transformation strategy

The table below presents the scope of work for design and implementation of proposed recommendations/ IT solutions/ applications, derived digital transformation strategy document.

Table 5: Scope of activities for Design and implementation of proposed recommendations/ IT solutions/ applications

Scope/ Timelines	Detailed list of activities
Project Planning **(1-2 months)**	Develop a Comprehensive Project plan and management approach containing sufficient details on work breakdown structure, sequencing, and period for every activity for implementation of proposed recommendations. The plan must include the staffing plan including numbers, roles, and responsibilities of team members. The plan must have a practical phasing of the development/ customization and configuration, testing, implementation, and rollout including project milestones and performance indicators that be used to monitor progress, and specific deliverables. The plan must also include: • the project management tool to be used (project management software or other tool(s)). • project communication plan. • project schedule, by item, and start and end dates. • methodology for various phases of project execution.

Scope/ Timelines	Detailed list of activities
	• risk management plan. • work breakdown structure. • schedule of project review, etc.,
Outputs at this activity: 1. *Detailed project plan* 2. *Project management approach document*	
System/ Application Design **(3-6 months)**	• Review existing as-is processes and systems and identify the gaps/ issues/ challenges • Review existing to-be processes and Functional Requirements Specifications (FRS) document for the proposed solution • Consultations with relevant department level stakeholders in finalizing to-be processes and functional requirements specifications document for proposed solution • Preparation of system requirements specifications for proposed based on the signed-off to-be process report (in case of bespoke development approach) • Solution gap analysis and customizations requirement assessment (in case of COTS application) and preparation gap analysis report • Obtaining sign-off on the requirements specifications report/gap analysis report • In case of proposed bespoke software development approach for the proposed solution, it is required to perform detailed System Design (using UML) for proposed solution including preparation of Logical and Physical Design, Logical Data Dictionary, and data/ file formats. Component and Deployment Views of the Application, Collaboration, and Class diagrams in the UML notations, Security and Features, Performance Features, Interface/ Control Design Features etc. and shall submit the System Design Document (SDD). • Consultations with relevant department level stakeholders on SDD report, incorporate the feedback and finalization of the SDD report
Outputs at this activity: 3. *System Requirements Specifications for proposed solutions based on the approved to-be process report including system integration/interfacing requirements (in case bespoke*	

Scope/ Timelines	Detailed list of activities
software development approach is followed) 4. *System Design Document (SDD) for the proposed solution (in case bespoke software development approach is followed)* 5. *Solution gap analysis report, including customization requirements (in case COTS approach is followed)*	
Development/configuration and customization **(6-8 months)**	• Implement the necessary hardware, system software, and application software as needed for development/configuration and customization of software as per signed-off System Requirements Specifications. • Perform the development/ customization and configuration of proposed solution based on the functional, system requirement specifications and designs finalized for the proposed applications/ solutions/ upgrades. • During the development/customization phase, it is important to conduct multiple conference room pilots for proposed applications/ systems to demonstrate the prototype of the solution and to obtain inputs on the proposed prototype. It should be avoided demonstrating the final solution without any interim reviews of prototypes of the system.
Outputs at this activity: 6. *Conference room pilots/demonstration of prototypes of proposed solution based on the agreed to-be process maps and system requirements* 7. *Design, development/customization, and configuration of solution/ application proposed*	
Software Testing **(3-4 months)**	• Design the software testing strategy including traceability matrix, test cases, and conduct testing of various components of the software developed/customized for proposed project. The software testing shall include full system testing including functional (*e.g., unit, integration testing*) and non-functional (*e.g., integration, performance, security, and stress testing*) etc., • Obtain the sign-off on testing approach and plan. • Perform the testing of the solution based on the approved test plan, document the results, and shall fix the issues identified during the testing. • Deploy necessary infrastructure and tools for conducting testing including integration, performance and shall

Scope/ Timelines	Detailed list of activities
	provide outputs of such tools for verification purposes. • Supply and implement necessary tools for tracking the bugs/issues/gaps identified during the testing. Particularly for performance, stress, and security testing during UAT, these tools shall be utilized and facilitate testing in consultation with the relevant stakeholders. • Provide formal approval for the test plan and to ensure that the product delivered meets all the requirements that are signed-off. • Engage a third-party quality assurance service provider to perform independent verification and validation of solution to assess the solution in various areas such as functionality, security, scalability, integration performance, etc., The acceptance testing, or any third party identified is for ensuring that systems provided meets the requirements • Provide and ensure all the necessary support or any third party in conducting the Acceptance Testing including providing access to system, sharing necessary project documentation, testing strategy, test cases developed for the applications/ solutions, test results, Action Taken report on issues identified during testing and relevant corrective actions taken, etc. • Address all the gaps identified during the acceptance testing, which will be revalidated by the third party/ government departments. • Deliver an error free solution upon addressing all the identified gaps and shall submit an action taken report for the issues reported during UAT.
Outputs at this activity: *8. Test strategy, test plans, test cases* *9. Test results* *10. Action taken report on issues identified during the acceptance testing and relevant corrective actions.* 11. *Fully tested, error free version of the software/ application*	
Documentation **(1-2 months)**	• Prepare/update the documents including that of To-Be reports, Functional Requirements Specifications, Systems Requirement Specifications, System Design Documents, Test Cases and Results, User Manuals, Training Manuals, Operational Manual, Maintenance Manuals, etc., as per applicable standards.

Scope/ Timelines	Detailed list of activities
	• Obtain the sign-off for all the documents and shall make necessary changes as recommended by the relevant stakeholder of departments before submitting the final version of the documents. • During the entire lifecycle of the project, it is to ensure that the project documents are kept up to date

Implementation and go-live for pilot phase
 	
(6-8 months)
	• Perform all required tasks to implement applications/ software and to make system ready for commencement of system usage by the users covered in pilot phase.
	• Activities to be carried out for implementation of applications/ software and go-live for pilot phase shall include
	  ○ *Implementation of IT infrastructure for production and DR instances*
	  ○ *Capacity building, communications, and change management services for pilot agencies*
	  ○ *Data migration for pilot agencies*
	• Upon successful transition to production environment and successful posting of real time transactions by users in applications/ software, the system shall be declared as 'go-live'

Outputs at this activity: *12. System go-live for pilot phase*	
System stabilization **(3-6 months)**	• Application/ System implementation for department/ government agencies can be envisaged to occur in a phased manner. The system shall be first implemented on a pilot basis (system stabilization period) for select agencies. • During system stabilization period, it is important to address all the issues identified in the system as per the timelines agreed in the SLA
Outputs at this activity: *13. Issue Log and Action Taken Report*	
System Rollout **(3-6 months)**	• Prepare a ***detailed plan for rollout of system***, in consultation with the relevant stakeholders, for all other agencies. The plan shall address sequencing of the

Scope/ Timelines	Detailed list of activities
	agencies for rollout, activities and timelines, roles, and responsibilities, etc., • During rollout, it is important to follow the below mentioned minimum set of activities: a. Preparation of necessary templates and documents to obtain information required from the line agencies to support in system rollout for respective agencies b. Conduct workshops and system walkthrough for select staff from the line agencies on system functionality and migration strategy (including details needed as per prepared templates) c. Coordinate with the spending agencies for obtaining the filled-up templates with the data required for system configuration for respective agencies d. System configuration[3] and workflow customization based on requirements provided by the spending agencies e. Configuration of users and authorizations f. Capacity building, communications and change management services for agencies covered in rollout phase g. Data migration for agencies covered in rollout phase • It is important to address any issues or gaps identified by the spending agencies during the rollout phase

Outputs at this activity:

14. Application/ System Rollout Strategy
15. Templates needed for obtaining information from spending agencies for system rollout
16. Workshops on system rollout for staff identified for support in system rollout
17. System configuration and customization for agencies covered in rollout phase
18. *System rollout for agencies covered in rollout phase including system rollout completion report for each agency*

c. Implementation of IT infrastructure to support the Digital transformation

In addition to the application and system software, it is also required to provide IT infrastructure related services including supply, installation, configuration, commissioning, operations, and maintenance of the related IT infrastructure for development, test, training, and production and disaster recovery instances. The table below presents the list of

[3] Computers shall be standardized to minimize investment in overcapacity in hardware.

activities for Implementation of IT Infrastructure to support the digital transformation strategy.

Table 6: Scope of activities for implementation of IT infrastructure to support the digital transformation strategy

Scope	Detailed list of activities
Preparation of IT infrastructure Implementation plan	Prepare a ***detailed plan for implementation of IT infrastructure***. The plan shall address the following at a minimum: • Final bill of material and specifications for each instance (development, testing, training, production, and DR instances) • Infrastructure delivery and implementation schedule for each instance • Roles and responsibilities of the stakeholders for IT infrastructure implementation • Deployment architecture including exact space required in DC/DR sites, rack placement plan in terms of floor layout plan, power requirements. • Network architecture • Security architecture • Installation and configuration plan including the IP addressing schema for IT infrastructure, etc., The IT infrastructure implementation plan shall be discussed and finalized in consultation with the relevant department stakeholders.
Outputs at this activity: *19. IT Infrastructure implementation plan*	
Supplying IT Infrastructure	• *Procure and supply the IT Infrastructure*, for all instances (development, test, training, production, and DR instances), based on final Bill of Material (BoM) and specifications included in the agreement. • Deliver the IT infrastructure for all the instances in good condition including all the transportation and logistics arrangements needed for the same. • The IT infrastructure supplied should be subjected to a third-party audit to verify the compliance of infrastructure with the BOM and specifications provided in the agreement and implementation plan. It is important to address any gaps identified during such audit at no additional cost.

Scope	Detailed list of activities
Outputs at this activity: *20. IT infrastructure delivery reports on (a) development and testing instances, (b) training instance, and (c) production and DR instances*	
IT Infrastructure Installation and commissioning	***Installation, configuration, and commissioning of the IT infrastructure*** for all instances at DC and DR sites. The personnel deployed for IT infrastructure installation and management at identified sites (both DC and DR sites) shall abide by the rules and regulations as applicable for respective sites. Any violation against the stipulated rules and responsibilities shall be treated severely and the concerned party should be directly liable for any loss or damage caused due to such violation and shall bear all the expenses for rectification of the same. Obtain necessary permissions from the relevant stakeholders for list of personnel to be deployed at these sites and only authorized personnel will be allowed to access the premises to carry out requisite tasks as needed. Follow a structured cabling and other industry standards for installation of the infrastructure. Upon completion of the configuration and installation, it is required to submit a detailed Installation report capturing the following: • Inventory of IT infrastructure including the make, model, serial number, system configuration, system software, related versions, etc., • Final infrastructure installation and configuration details, etc., The IT infrastructure installed should be subjected to a comprehensive third-party validation covering performance, security, and availability testing to verify whether the installation is complete, and it meets the requirements The gaps identified during third party validation and testing should be address to the satisfaction of the relevant stakeholders and should submit an Action Taken Report detailing the status of each gap/issue reported during third party validation and testing.

Scope	Detailed list of activities
Outputs at this activity: 21. *IT infrastructure installation reports (one report for development and testing instances, one report for training instance and one report for production and DR instances.* 22. *Action Taken Report (s) detailing the resolution provided for gaps identified in third party validation and testing of IT infrastructure*	

d. Capacity building, and Change management services

This section discusses the scope of services to be provided by SI for building necessary capacities and skillsets in the stakeholders, during pilot, and rollout phases, to support in usage, operations, and maintenance of IT application software and associated IT infrastructure. The table below presents the scope of work for System Integrator (SI) for capacity building (incl. training) and change management services.

Table 7: Scope of activities for Capacity building and Change Management services

Scope	Detailed list of activities
Preparation of Training Plans	During the implementation phase, it is important to prepare a ***detailed training plan*** including training program, detailed training curriculum, delivery methods, schedules, and locations for training, roles, and responsibilities for conducting the training programs covering training requirements for pilot and rollout phases.
Outputs at this activity: *23. Training Plans*	
Development of Training Material	The training programs shall be developed and conducted in English/ Local Language. Training programs should be conducted instructor led training programs and following minimum training material should be provided for each participant in the training program: • Course content in hardcopy and softcopy • Participant handouts/handbook For train the trainer programs, in addition to the above material, it is required to provide following additional material to the participants: • Trainer handbook, detailing the guidance and instructions on conducting respective program • Course evaluation tools

Scope	Detailed list of activities
	For end user training on application software, it is also required to develop the following training materials to support the stakeholders in self-learning: • CBTs on system operations and usage • Online help and user guides All the training material developed should be made available for registered and authorized users in the portal.
Outputs at this activity: 24. *Training material*	
Conduct training programs	Conducting the training programs as defined and finalized in training plan during pilot and rollout phases. Conduct additional programs for each training course as per emerging needs of the project. For each training program conducted, a training completion report shall be prepared and submitted to relevant stakeholders, covering the details and schedule of training program, target participants, findings from training program, etc., Based on the initial training programs conducted and feedback received from the participants, the training material should be updated and submitted to relevant stakeholders, addressing the feedback/concerns identified by the participants, if any.
Outputs at this activity: *25. Training completion report for each training program* 26. *Updated Training Material*	
Clarifications support during rollout of training programs	Provide clarifications support on a continuous basis for training programs conducted by the trainers from train the trainer programs. Such support may cover providing necessary clarifications to the trainers on course content, coverage, functional and technical aspects delivered through the training course etc.
Deliverables: *27. Clarifications and advisory support for rollout of training programs*	

Scope	Detailed list of activities
Development of Change Management & Communications Strategy	Perform following minimum tasks for development of the strategy: • Assess the impact of system implementation on the legal framework, processes, organization structures and systems • Assessment of the impact of the changes in processes, structures, and systems on the stakeholders, both internal and external • Review the level of preparedness of stakeholders to implement and rollout • Conduct necessary consultations with all categories of stakeholders to identify their concerns and to develop a suitable plan to address these concerns. This will require the change management team to travel to the select offices with in Chennai, other regions, and divisions of the State to understand the specific issues and concerns at respective levels. • Development of a comprehensive change management strategy and implementation plan for addressing the people related concerns aspects in system implementation and to minimize the impact of changes to enable successful adoption of the system • The change management strategy and implementation plan shall include the short-, medium-, and long-term measures for ensuring successful adoption of systems by the stakeholders. • Ensure that the strategy and implementation plan are updated based on the learnings in implementation of the same • Prepare and implement a comprehensive communications plan covering all stakeholders who are impacted by transformations. The communications plan must identify the key audiences, their associated information needs, the most suitable method of communication and suggested content and frequency of communications. The communications plan must anticipate leveraging internet/intranet and other suitable technologies (including mobile devices, e.g., phones, tablets) for maximizing the reach and it is expected to develop/supply and implement such technologies and content for such purposes and to maintain the currency of the information and content disseminated through such technology during project period. This plan must be reviewed and updated frequently to improve its effectiveness and ensure changes in needs are incorporated and reflected in current plan • Prepare and make necessary presentations on the developed change management and communications strategy and implementation plans and shall update the documents based on the feedback provided by relevant stakeholders.

Scope	Detailed list of activities
Outputs at this activity: *28. Change Management Strategy & Implementation Plan* *29. Communications Management Strategy and Implementation Plan*	
Implementation support for change management and communication strategy/plans	Provide necessary support in implementation of the signed-off change management and communications management strategy/plans including the following activities: • Development of necessary content/material for conducting the change management and communications workshops • Conducting the change management workshops for the stakeholders within Chennai and other regions as per agreed change management strategy/plan • Designing and developing the content required for implementation of communication measures (workshops, online content in the portal, mailers, banners, e-mails, audio-video presentations, etc). • Keep the content updated based on the implementation progress. • For communication measures apart from workshops and portal, the responsibility of the system integrator is to design and development of the content, along with Printing, distribution and presenting the content to the stakeholders. • For online/electronic content to be disseminated through portals, design, develop, and host the content in the portal and to keep it updated based on implementation progress. • Conduct 'Train the Trainer programs' for the staff identified in conducting the change management and communications workshops for other staff in their respective departments/agencies. • Based on feedback received from participants during change management workshops, train the trainer programs and implementation of communication measures, it is important to update the content/material for change management workshops/communication measures and shall submit the same.
Outputs at this activity: *30. Content/material for rolling out change management workshops and other communication measures agreed in the strategy/plan* *31. Change management workshops and train the trainer programs* *32. Updated content/material for change management workshops and communication measures*	

Scope	Detailed list of activities
33. Hosting content in portal for communication requirements of stakeholders	

e. Data digitization and migration

This section discusses the list of activities for digitization and migration of data required for digital transformation strategy's implementation:

Table 8: Scope of activities for Digitization and migration of data services

Scope	Detailed list of activities
Development of Data Digitization and Migration Strategy	Based on the detailed requirements specifications signed-off for various functions and modules covered during implementation, detailed assessment of data digitization and migration requirements for each module is to be done. A detailed data digitization and migration strategy capturing the specific data elements needed, source data for each data element, data conversion and migration plan, roles and responsibilities of stakeholders must be prepared. Define the data quality criteria, as part of data digitization and migration strategy, for data elements required for implementation of various modules and which are expected to be digitized by the oversight, government agencies using the formats provided. Digitizing old documents into searchable and usable document formats should be done after a common standards/ templates are evolved. After the standards/ templates are evolved, the digitization activities may be taken up for a period of past 10 years.
Outputs at this activity: *34. Data digitization and migration strategy*	
Development of templates for data preparation	For the data, which need to be digitized, it is required to provide necessary templates for providing such data by the oversight, revenue, and spending agencies. The templates shall be developed in MS Excel or similar tools to enable the spending agencies to provide the data and such templates shall include inbuilt controls to ensure that complete and appropriate data is captured by the oversight, revenue, and spending agencies. For the data available in electronic format or in the existing information systems, it is advised on specific data elements, format, and structure in which the data need to be extracted from the existing system and to be provided for migration.

Scope	Detailed list of activities
Outputs at this activity: *35. Templates for preparation of data by the government agencies*	
Coordinate with oversight, revenue, and spending agencies for obtaining data	Coordinate with the respective resources identified by oversight, government agencies for obtaining the filled-up templates for data, which need to be migrated to new/ updated systems/ applications. Prepare and submit status reports to relevant stakeholders on submission of filled up data formats by the agencies. Any delays in receiving the filled-up data formats should be escalated in a timely manner through status and escalation reports.
Outputs at this activity: *36. Status Reports* 37. *Escalation Reports for delays in receipt of filled up data formats*	
Data Quality Assessment and Reports	For the filled-up data formats provided by the agencies, it is important to perform data quality assessment using necessary tools and scripts to validate the digitized data against the defined data quality criteria for respective modules. Prepare/generate a report on data/records not complying with the defined data quality criteria and shall submit the same to the respective agency for corrections.
Outputs at this activity: 38. *Data Quality Assessment Reports*	
Data Migration	Upon completion of data quality assessment and necessary corrections in data by respective agencies, it is important to perform data migration. The data migration activity performed should ensure that the data is migrated completely and accurately. Design and implement necessary validation checks and controls to ensure that migrated data is accurate and complete in comparison to the data provided by respective agencies. Based on the data migration activities completed for each agency, it is required to submit status reports on data migration for each agency.
Outputs at this activity: *39. Migration of updated and corrected data*	

Scope	Detailed list of activities
40. *Data migration status reports*	

In addition to the abovementioned scope of services, it is also important to consider the aspects such as providing warranty, operations, and maintenance services for solution including all the software and hardware components from the date of operational acceptance of the solution and such services shall be provided throughout the contract period. The warranty for IT infrastructure supplied and implemented for development and test instances should be valid from the date of implementation and acceptance of such and should be valid.

This section discusses the warranty, operations, and maintenance. It is important to have a back-to-back arrangement with the OEMs (for all software, hardware components, and any other items supplied during the contract period) for warranties for the entire contract period. The validity of this agreement with all OEMs shall continue in the event of any extreme and unforeseen circumstances, at any time after implementation, for any reason whatsoever.

f. Establishment and management of Helpdesk Operations

It is required to establish helpdesk for supporting the system users in day-to-day operations. The staff of helpdesk shall provide systems support, recording, and addressing the system issues reported by the users on usage, functionality, transactions, system performance etc. The following table presents the list of activities for establishment and management of helpdesk.

Table 9: Scope of activities for establishment and management of helpdesk operations

Scope	Detailed list of activities
Establishment and Management of Helpdesk Operations	a. Implement a central Helpdesk, with minimum defined/ agreed number of helpdesk staff, for recording the issues reported by the users and to provide the resolution for the technical/functional issues. The central helpdesk shall be operational from defined/ agreed number of hours on working days. The central helpdesk shall act as a coordination point for reporting the end user issues related to products and services provided. The staff at helpdesk during the prescribed times above should always be minimum five and resource loading should consider the leave and holidays of the staff. The resources deployed in the helpdesk should be able to speak English and Local language (Tamil) fluently. b. Based on the emerging needs, it is important to deploy additional resources for the helpdesk to support in increasing volume of transactions and related support needed for system users. It may vary the composition (no. of resources) of the helpdesk at any point of time during the maintenance phase.

Scope	Detailed list of activities
	c. Provide necessary IT and support infrastructure as needed for helpdesk including computers, printers, scanners, telephones, etc., d. It is to be noted that government departments may decide to deploy its own resources for recording the issues reported by the staff and such issues may be allocated for issue resolution. e. The physical space for establishment of helpdesk will be provided by government agencies (including necessary supporting infrastructure (non-IT), network connectivity from helpdesk to the data centre and disaster recovery sites). f. Other IT infrastructure needed for helpdesk staff and related operations shall be supplied and implemented. g. Establish hot-line number for the helpdesk team and the capital and operational expenditures for the telecommunication services (*except for bandwidth cost between helpdesk and DC/DR sites*) by the concerned stakeholders. It should be ensured that these numbers are operational and available. h. Implement the Helpdesk management system, to record and track the issues reported by the end users and to monitor the efficiency of the services offered to the users. i. Access to the helpdesk management system shall be provided to all the users and it should facilitate in reporting the technical issues/ problems, which requires support from helpdesk. j. Issue categorization approach for categorising the reported issues into Severity 1, 2 and 3. The issue resolution support for Severity 1, 2 and 3 issues shall be provided in line with the timelines indicated in defined/ agreed SLA. k. The helpdesk support shall also include e-mail-based support. This will include creating a dedicated email address for support required for users. The e-mail support will be used by the users for reporting errors, logging system issues or for any other support needed for operations. Helpdesk support staff is required to log the issues reported through email in the helpdesk management/call log management system and shall provide the user with the issue tracking number. Support staff shall provide timely support to address the issues reported/support sought by the internal employees. l. Based on helpdesk operations, it is important to submit the performance reports on helpdesk operations including number of calls reported, number of calls resolved within and outside the agreed KPIs, etc. It is important to submit such reports on a weekly/fortnightly/monthly basis.

g. Warranty, and Maintenance Support of Application and System Software

This section outlines the overview of warranty, operations, and maintenance services to be provided for application and related system software implemented. The warranty, operations and maintenance for application and system software includes, but not limited to, ensuring defect free operation of the systems, systems monitoring, troubleshooting, and addressing the functionality, availability, and performance issues, implementing the system change requests etc. It is important to keep the application software in good working order; perform changes and upgrades to applications. It is important for addressing all the defects identified by the users during the support period. The operations and maintenance support shall be for a specified period from date of go-live for pilot. The operations and maintenance support services shall conclude on the date of O&M support conclusion. Warranty for the hardware delivered and implemented during the contract period should be valid for a period of three years from the date of commissioning and acceptance of the hardware or its sub-components.

Table 10: Tentative duration for warranty and support period

Category	Duration
Warranty and Support	For a specified period from commissioning and acceptance of pilot phase
Warranty and Support	To commence from date of commissioning and acceptance and to conclude with the closure of O&M support

The following is the broad scope for maintenance and support functions about the software.

Table 11: Scope of activities for warranty and maintenance support of applications and system software

Scope	Detailed list of activities
Compliance to SLA	Ensure compliance to uptime and performance requirements of solution as per the defined performance requirements and any upgrades/major changes to the software shall be planned accordingly for ensuring the SLA requirements
Application Software Maintenance	Address all the errors/bugs/gaps in the functionality offered by solution (*vis-à-vis the FRS and SRS signed off*) at no additional cost during the operations and maintenance period. The warranty and maintenance support for application software shall include minor changes identified to the software during the operations and maintenance phase. The minor changes to the software shall include, but shall not be limited to, the following: *a. Changes to the user interface/form layouts* *b. Changes to the user workflow/approval processes*

Scope	Detailed list of activities

c. *Changes to the parameterized values (e.g., changes to the tax rates, applicable deductions for payments to be made to employees, suppliers, creditors)*
d. *Changes to the report layouts, etc.,*

The above-referred software changes shall be undertaken by the SI as part of application warranty and maintenance support.

For major software changes required during the contract period, due to changes to acts, regulations, guidelines and procedures, government departments should submit software requirements.

Based on requirements provided, it is required to assess efforts and timelines required for implementation of proposed change and shall submit a formal change request with such details including resources, timelines, and total man-month inputs required for implementation of the change request. The effort estimates provided for change request should be reviewed and finalized.

Based on agreed total man-month inputs required for the change request and the blended man-month cost quoted, the total cost for implementation of change request shall be agreed and signed-off.

Payment for change request should be made upon successful implementation of the change request and conclusion of user acceptance testing successfully.

Upon sign-off on effort and cost estimates for implementation of change request, it is important to perform requisite tasks for implementation of the change request including design, development/customization, testing, and implementation of such enhancements/ software changes in the test instance.

Departments should conduct user acceptance testing for such changes implemented and upon satisfactory conclusion of UAT, the changes shall be migrated from test instance to production instance.

Another round of testing shall be performed by government departments in production environment and upon satisfactory conclusion on implementation of change request.

Departments should issue an acceptance certificate for implementation of the change request. Based on the acceptance certificate from government departments, it is important to submit an invoice to government agencies based on signed off cost estimates for

Scope	Detailed list of activities
	implementation of such change request. Any changes/upgrades to the software performed during the operations and maintenance phase shall be subjected to the testing to ensure that the changes implemented in the system meets the desired and specified requirements and does not affect any other function of the system.
Database Management	Performance management of the database systems and servers implemented including continuous monitoring of the performance of the system, ensuring system performance in line with the defined SLA etc.
Problem identification and Resolution	Identification and resolution of application problems (e.g., system malfunctions, performance problems and data corruption etc.)
Software Change and Version Control	All planned changes to application systems shall be coordinated within established Change Control processes to ensure that: *a. Appropriate communication on change required has taken place* *b. Proper approvals have been received* *c. Schedules have been adjusted to minimize impact on the production environment* Define the Software Change Management and Version control process and obtain approval for the same. For any changes to the software, it is important to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. It is also required to obtain approval for all the proposed changes before implementation of the same into production environment and such documentation is subject to review at the end of each quarter of operations and maintenance support.
Maintain configuration information	Maintain version control and configuration information for application software and any system documentation
Maintain System documentation	Maintain and update documentation of the software system. Ensure that: *a. Source code for the customizations is documented* *b. Functional specifications are documented* *c. Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS/ To Be report, in accordance with the defined standards* *d. User manuals and training manuals are updated to reflect on-going*

Scope	Detailed list of activities
	changes/enhancements e. *Standard practices are adopted and followed in respect of version control and management*

h. Warranty, and Maintenance Support of IT Infrastructure

The following outlines the overview of warranty, operations, and maintenance services to be provided for IT infrastructure supplied and implemented at the data centre and DR site.

Table 12: Scope of activities for warranty and maintenance support for IT infrastructure

Scope	Detailed list of activities
General Services	• Provide a comprehensive warranty for the infrastructure supplied and warranty should be valid throughout the contract period. Warranty referred here means that the Products supplied will remain defect-free, and any remediation of any defect that arises in this period will be the responsibility of the third-party agencies and costs of such remediation will be borne by the third-party agencies. • Overall monitoring and management of the systems implemented in the DC and DR sites, which includes administration of Infrastructure (Web/application servers, database servers etc., and all other services ancillary to these facilities to ensure performance and availability requirements of the Project. • The system for monitoring and administration of the IT infrastructure implemented should be supplied and implemented. Such system shall also support in monitoring the defined/ agreed SLAs • 24x7 monitoring and management of availability and security of the infrastructure and assets through the Enterprise Management Solution implemented. • Design and Implementation of a comprehensive security policy in respect of the digital systems and assets conforming to ISO standards • Ensuring uptime, performance, and other key performance requirements including data backup and business continuity • Design and implement adequate data backup and restoration procedures (including the database, attachments and all other data elements created in and generated by the system and users). • Ensure that Data backup is maintained until the last transaction occurring in the system • Perform the patch management, testing, and installation of software upgrades issued by the OEM/vendors from time to time. These patches/upgrades, before being applied on the live infrastructure of the data center, shall be adequately tested. Any downtime caused due to upgrades and patches shall be taken into

Scope	Detailed list of activities
	to the account and it shall not be considered as 'Agreed Service down Time'. • Application of anti-virus polices/patches for the IT infrastructure • Develop the Standard Operating Procedures (SOPs), in accordance with the ISO and ITIL standards, for management. These SOPs shall cover all the aspects including Infrastructure installation, monitoring, management, data backup and restoration, security policy, business continuity and disaster recovery, operational procedures etc. • Obtain signoffs on the SOPs from the departments and shall make necessary changes, as and when required, to the fullest satisfaction of departments. • Adopt the agreed SOPs during the service transition and operation phases covering the major service management processes. • Preventive maintenance, carrying out the necessary repairs and replacement of parts wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be attended during working hours, unless inevitable and approved. • Reactive maintenance that is intended to troubleshoot the system with sufficient teams • Performance tuning of the system as may be needed to comply with SLA requirements on a continuous basis. • Continuous monitoring and management of IT infrastructures during the defined working hours and restoration of breakdown within prescribed time limits • Monitoring security and intrusions into the system, which include taking necessary preventive and corrective actions • Monitor and record server performance and take corrective actions to ensure performance optimization daily. • Escalation and co-ordination with other vendors for problem resolution wherever required • System administration tasks such as managing the access control system, creating, and managing users, taking backups, task, and batch processing etc. • Ensure that daily back-up copies of the data are created and maintained safely • Whenever a component must be replaced because of technical, functional, manufacturing or any other problem, it shall be replaced with a component of the same make and configuration. In case the component of same make and configuration is not available, the replacement shall conform to open standards and shall be of a higher configuration and shall be approved. • Produce and maintain system audit logs on the system for a period agreed. On expiry of the said period, the audit logs should be

Scope	Detailed list of activities
	archived and stored off-site at a location agreed. • A log of issues raised at the help desk should also be maintained similarly and produced periodically • Regular review of the audit logs for security lapses. • Review security advisories (such as bulletins generally available in the industry) on a regular basis to determine vulnerabilities relevant to the IT assets and take necessary preventive steps. • At the end of the contract period or during the contract period, if any other agency is identified for providing O&M Services for IT software, SI selected through this bid is required to provide necessary handholding and transition support, which shall include but not limited to, conducting detailed walk-through and demos, handing over the entire software (including source code, program files, configuration files, setup files, project documentation), addressing the queries/clarifications of the new agency, conducting training sessions. • As part of this support, develop and implement the Information Systems Security Policy (ISSP) and procedures in compliance with ISO standards, for managing the Security of Information Systems. The ISSP including procedures shall be validated by the third party and gaps identified during such review shall be addressed to the complete satisfaction. It is important to implement such security policy for operations and maintenance of IT systems and other IT infrastructure supplied and implemented. • Reactive and proactive maintenance support for IT infrastructure • Maintenance of necessary spares as required for the IT infrastructure supplied to ensure uptime of the systems
User Profiles and Account Management	• It is required to design and implement the user management processes including creation of a domain, user/group profiles in a manner, which ensures that the end users are provided only with specific privileges required for designated operations • The user-id naming and protocol shall be designed and implemented for all the user ids. Such naming convention and protocol shall be signed-off, which shall be adopted across the country • Necessary user account creation, management policies, and procedures shall be defined and implemented including obtaining approval for each user id created in the system. Separate user id shall be created or each employee, which uniquely identifies that employee in the system • The end users shall only be provided with role-based privileges and access. Such roles, privileges shall be signed-off • System administration tasks such as managing the access control system, creating, and managing users etc.

Scope	Detailed list of activities
	• Enable audit logs for the server/system activities and such audit logs shall be analyzed at regular intervals to identify and address the security and performance issues • Produce and maintain system audit logs on the system for a period agreed. On expiry of the said period, the audit logs should be archived and stored off-site
Data Backup Management	• Designing and implementing a comprehensive data backup management solution at the DC and DR sites. The IT Infrastructure required for Storage and data backup requirements at DC and DR site shall have to be supplied by the SI accordingly. The data backup management requirements shall be comprehensively including maintaining the server image backups, to facilitate quick restoration of the systems from any unforeseen event • Design a detailed Data management policy, which highlights the SOPs for data storage, data backup and retrieval including frequency and processes of data backup management, type of backup (incremental or full) to ensure that all the data related to IT systems is available in the storage solution and is also available in a backup media/solution • Configuration, implementation and ensuring the data backup and replication between the DC and DR sites • Ensure that the tapes/DVDs are in operational condition and shall perform the tests to restore the data from the data backup tapes monthly. Such restoration tests carried out monthly shall also be recorded in a register • Data backup tapes shall be labeled appropriately and stored in the custody of the government agencies. • Maintain the Data backup activity register for each facility identifying the data backup activities performed, date of obtaining the data backup etc. • Maintain the manual registers for the data backup activities carried out at DC/DR site. • Enable the necessary audit trails on the IT infrastructure at DC/DR site, which track the data backup and restoration activities. Such registers/audit trails shall be verified for measuring the performance of SI against the defined SLA. • Ensure that daily back-up copies of the data are created and on a weekly basis the entire data backup on the external storage tapes shall be kept/updated in the location agreed with the government agencies

Scope	Detailed list of activities
IT Infrastructure Asset Management	• Design and implement the processes and procedures for effective asset management for IT infrastructure implemented in DC and DR sites. Government agencies shall review such processes and procedures defined based on the gaps identified in the processes will make necessary changes. In line with the signed-off asset management process, SI shall maintain the Asset Registry for all the IT and supporting infrastructure including the part numbers/serial numbers, configuration, changes made to the asset in terms of replacements/upgrades etc. Such asset registers and information shall be maintained. • Ensure that such documentation is kept up to date and is available to government agencies for verification and review at any point of time during the contract. Submit a quarterly Asset Information Register to government agencies with the updated and current information.
Transition Management	• At the end of the contract period or during the contract period, if any other agency is identified for providing Operations and Maintenance Services for IT application and IT infrastructure, SI selected through this bid is required to provide necessary handholding and transition support to the complete satisfaction. • The ownership of the assets (including soft and hard components existing and procured through this tender), at any point of time during the contract or expiry of the contract, shall rest with the Government. • During the contract period, ensure that all the documentation including policies, procedures, asset registers, configuration documents are kept up to date and all such documentation is handed over during the exit management process

6.2 Standards and Regulations for Building Blocks

6.2.1 Business Architecture Standards

Table 13: Business Architecture Standards

S.No.	Standards	Recommendations
BS.1	**Business Process Modelling**: Business Process Model and Notation (BPMN) is a standardized notation for depicting business processes in a workflow for any organization. The primary goal of BPMN is to provide a standard notation that is readily understandable by all business stakeholders.	Must be followed for all business process modelling. Teams must use standard tools.

BS.2	**Architecture Modelling Language**: Unified Modelling Language (UML) would be used for designing systems, architecture designs and other modelling. UML is a language for specifying, constructing, visualizing, and documenting the artefacts of a software-intensive system. It is a general-purpose modelling language used with all major object methods and applied to all application domains.	Future state recommendations post 1st phase roll-out of Digital Tamil Nadu. The UML/other modelling standards require socializations before acceptance.
BS.3	**Digital Service Standard**: Digital Service Standards would be mandated to ensure departments are planning delivery of e-services consistently across the Government of Tamil Nadu Departments.	Must be adhered to for service designing. All services would go through Tamil Nadu Service Assessment Framework for approval for implementation
BS.4	**Design Thinking:** Human-centered design for interactive systems (ISO 9241-210:2010) - It provides requirements and recommendations for human-centered design principles and activities throughout the life cycle of computer-based interactive systems.	Must be followed for all design thinking standards
BS.5	**Accessibility**: Web Content Accessibility Guidelines (WCAG) (Level A, AA, AAA) - The WCAG documents explain making web content more accessible to people with disabilities	Must be followed for all web content accessibility guidelines and standards

6.2.2 Application Architecture Standards

Table 14: Application Architecture Standards

S.No.	Standards	Recommendations
AS.1	User Interface Standards	Adherence to GIGW standards for user interface design
AS.2	Code Readability	Indent and comment on code for better readability
AS.3	Web Service Standard	Follow latest standard of protocols such as SOAP ✓ JSON ✓ XML ✓ Web Services Interoperability (WS-I) ✓ Web Services Description Language (WSDL) ✓ Web Services Inspection Language (WSIL) ✓ Universal Description, Discovery, and Integration (UDDI)
AS.4	Code Naming Convention	Use of Camel Case and business relevant name in declaring all classes, entities, and variables
AS.5	Software and System Engineering	Follow ISO/IEC/IEEE 24765 standard for systems and software engineering
AS.6	Software Testing	Follow ISO/IEC/IEEE 29119 standard for software testing

6.2.3 Data Architecture Standards

Table 15: Data Architecture Standards

S.No.	Standards	Recommendations
DS.1	**Metadata and Data Standards** Refer Metadata section in this document	State-wide metadata standards have been illustrated in subsequent section
DS.2	**Location Codes**: Standard location codes with a mechanism for dynamic update of create/split/merger of villages/blocks/districts/states and local governments.	Refer GoI LGD Codes
DS.3	**Open Data Element**: To define Object-oriented	Refer data.gov.in for data catalogues

	classification of data elements based on Open Group Framework	and Open Data policy (NSDAP)
DS.4	**Data Naming Convention**: Follow SQL Server Naming Convention or Hungarian notation.	This is a mandatory standard and must be defined, agreed, and followed

6.2.4 Technology Architecture Standards

Table 16: Technology Architecture Standards

S.No.	Standards	Recommendations
TS.1	**Simple Network Management Protocol (SNMP):** For collecting and managing information about managed devices for the network, the standard protocol to be used is SNMP. SNMP forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). Network management systems use SNMP to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including application layer protocol, a database schema, and a set of data objects. SNMP (preferably latest version) would be used Digital Tamil Nadu as a standard.	Must adhere for implementation of managed devices
TS.2	Internet and Intranet Access Browser/ Mobile – Browser: Support latest versions of widely adopted browser(s) including ✓ Internet Explorer (IE) ✓ Chrome ✓ Firefox ✓ Safari ✓ Opera	Must be adhered while developing and implementing new systems
TS.3	Storage and Backup Networked Attached Storage (NAS): Support Ethernet (IEEE 802.3) for NAS.	Must be adhered to ensure standards compliance at the time of procurement
TS.4	WAN, LAN, WLAN, all technology components: All devices in LAN and WAN infrastructure shall support IPv6 standards (128 bits for addressing).	Must be adhered to ensure standards compliance at the time of procurement of network devices
TS.5	WAN Network Communication Devices: Support Open Shortest Path First (OSPF), OSPF2, Multi-path OSPF for core switch.	Must be adhered to ensure standards compliance at the time of procurement of network devices
TS.6	WAN Network Communication Devices/ Network Security Devices: Support Secure Sockets Layer v3 (SSLv3) for mutual authentication between a client and server. Support SSH for secure remote login, secure file transfer and secure TCP/IP and X11 forwarding.	Must be adhered to ensure standards compliance at the time of procurement of network devices
TS.7	Secure Shell (SSH) and SSH File Transfer Protocol (SFTP): Network Protocol for information exchange - SSH would be used as the default standard for information exchange. Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. SFTP would be used as the default standard for content exchange. It runs over the SSH protocol. It supports the full security and authentication functionality of SSH.	All system must adhere to the standard
TS.8	Internet Protocol v6 (IPv6): IPv6 would be used as the default standard. IPv6 is the next generation protocol to replace the current version, IPv4.	This standard is a future state recommendation, however, it recommended to implement the

		standard for new implementations
TS.9	Domain Name Service (DNS): DNS would be used as the default standard for Network Domain Service. DNS stores and associates many types of information with domain names; most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail exchange servers accepting e-mail for each domain.	Default standard, must be adhered

6.2.5 Standards for Privacy and Security

Citizen's privacy is an important consideration that needs to be incorporated in the overall design and implementation of the TNEA. The standards and various operational requirements for privacy and data security are specified as follows for adherence:

- ✓ Security - Digital Certificate, TLS /SSL, SHA-256, AES-256
- ✓ Access Control - ISO 22600:2014 informatics - Privilege Management and Access Control
- ✓ eSign – online electronic signature service that will be integrated with service delivery applications via an API to enable user to digitally sign a document.

6.2.6 Technical Interoperability

Interoperability Standards defined by lndEA Framework shall be adopted by all systems constituting the State level service delivery.

- ✓ Seeks to connect varied systems developed using different technologies and on different platforms.
- ✓ Standards should be agnostic to underlying infrastructure relating to computing, storage, and network. Implementers should be able to incorporate standards on top of their existing solutions.
- ✓ TNEA recommends a federated architecture for collecting and classifying & owning services information. While certain core datasets like registries, would be managed centrally, the bulk of information relating to citizen service records would be maintained and managed in a distributed model, i.e., at state/district/local levels.

Note: For more information, refer the Reference Standard Document for Data and Cyber Security V 1.0 developed by Department of Information Technology, Govt. of Tamil Nadu, dated November 2021.

6.3 Architectural, design and operational recommendations

Metadata and Data Standards (MDDS) requirements ensure a common understanding at the semantic level. They ensure correct, proper use and interpretation of the data by its owners and users. Government of India e-governance standards[4] provide a set of recommendations

[4] http://egovstandards.gov.in/

for creating, interoperating, and using electronic service record systems within an enterprise and external ecosystem at various levels.

Inter-operability at the technical level requires specific integration solutions. Inter-operability at the institutional level requires a dialogue between Government organizations to understand information needs, as well as barriers to better quality and use of information. Overcoming such semantic and technical barriers are necessary for the government to achieve interoperability.

6.3.1 Minimal Data Elements

Various Governments have taken the initiative to design the metadata model and derive the standards. The successful among those were the ones that designed a minimal metadata model and subsequently built on it. For Tamil Nadu State Level Enterprise Architecture, a similar model could be adopted as Minimal Data Elements.

A minimal set of metadata elements would be designed at the state-wide level, while each departmental system would have the mandate to follow the model and the flexibility to augment the model as and when required.

6.3.2 State-wide Minimal Metadata Elements

The Tamil Nadu State Level Enterprise Architecture Metadata Structure defines the metadata elements. It also defines the reference metadata to be collected or reported by specifying the concepts required, how they relate to each other, their presentational structure, and which objects they are to be attached.

- ✓ Title/Name – Name given to the data element.
- ✓ Description – A description of the data element and its spatial, temporal, or subject coverage.
- ✓ Format – File format, physical medium, dimensions of the resource, or hardware and software needed to access the data. (As per GoI MDDS this also means – Char/Varchar, Integer, Date type)
- ✓ Identifier – A unique identification assigned to the data element.
- ✓ Relation – A reference to an available data element
- ✓ Data Steward – The entities or persons who hold the rights to the data element.
- ✓ Classification – Information about the rights held in and over the data element.
- ✓ Contact Information – Identification and means to communicate with persons or entities associated with the data.

6.3.3 Metadata Standards

This TN State Level Enterprise Architecture metadata standard need to be defined which would describe the metadata elements that the Government of Tamil Nadu's agencies

(departments/directorates/sub-organizations) should adopt to describe the different entities involved in their business and records management processes. It is to be designed to describe not only records but also other entities (agents, business, and mandates) that provide the necessary context within which records exist and operate, and the relationships between them. Adopting this standard will enable management of access to and understanding the records that document an agency's business over time.

6.3.4 Operating Model

Figure below gives the typology of metadata standards along with the state-wide standards. The agencies under the Government of Tamil Nadu must adopt the state-wide standards or seek architecture exceptions for adoption. The agencies may add any additional standard based on their specific need of the domain.

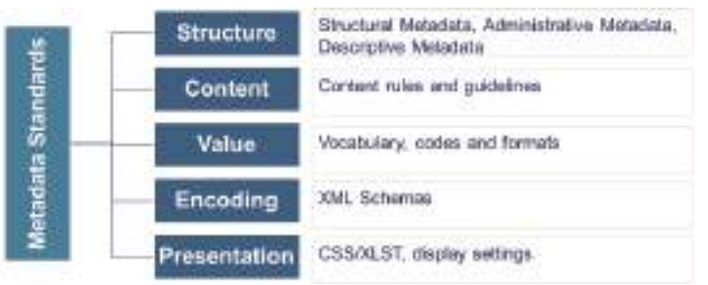


Figure 9: Metadata Typology

6.3.5 Structure related Standards

Table 17: Metadata Structure standards

Description	Mandatory/ Optional	Reference	Remarks
Minimal Metadata Elements	Mandatory	MDDS - http://egovstandards.gov.in/metadata-and-data-standard	Follow Government of India, MDDS standard for details around each metadata element
DDI: Data Documentation Initiative	Optional	https://ddialliance.org/explore-documentation	Applicable for surveys and other observational methods in the social, behavioral, economic, and health sciences

Table 18: Metadata Content standards

Description	Mandatory/ Optional	Reference	Remarks
National spatial data infrastructure standards	**Mandatory**	https://nsdiindia.gov.in/nsdi/nsdiportal/images/NSDIMetadataDocument.pdf	Applicable for GIS data definition and exchange format

Table 19: Metadata Value standards

Description	Mandatory/ Optional	Reference	Remarks

Local Government Directories	**Mandatory**	GoI LGD - https://lgdirectory.gov.in/	In line with GOI guidelines - Applicable for districts, blocks, and villages
Agency/ Department Codes	**Optional**	Need to form	All agencies need to be codified with unique code and standardized
W3CDTF Data and Time Format	**Optional**	http://www.w3.org/TR/NOTE-datetime	Data and time format of for all applicable entities not covered in MDDS

Table 20: Encoding related standards

Description	Mandatory/ Optional	Reference	Remarks
Encoding and transmission format	**Optional**	http://www.loc.gov/standards/mets/	-
Extensible markup language (XML)	**Optional**	https://www.w3.org/XML/	-
XML schema for generic data elements: Specific to land region codification	**Mandatory**		This standard is aligned with LGD

6.4 Policy Recommendations

In Addition to the Standards and Regulatory Framework, State shall develop or repurpose existing policies:

- ✓ Structure of Transaction Records and Indexes to be maintained at State level
- ✓ Policy for digitization of legacy or non-standardized (free text/paper) records
- ✓ Policy for storing heavy records (scanned data)
- ✓ Policy for emergency access and use of data for research and analytics
- ✓ Policy for record retention, discarding and archival
- ✓ Policy for data privacy and security
- ✓ Policy for code dictionary updating

6.5 Architectural Approach

6.5.1 Business Architecture

Business architecture will follow current state service identification, rationalization of services, prioritization of services, service catalogue finalization and plan to implement the re-engineered services.

1. As-Is State Service: Services must be captured that are already delivered by various departments
2. Service Rationalization: Services must be subsumed under relevant service domains and rationalized

3. Service Prioritization: The parameters identified are elaborated below:
   - ✓ Maturity Level of service as per Digital Service Standards (DSS): Basis DSS assessment framework service maturity must be identified as per DSS defined by MeitY (Refer http://egovstandards.gov.in/notified-standards-0)
   - ✓ Complexity of Implementation: The viability of delivering the service value completely through digital technologies will be considered
   - ✓ Value to Stakeholders: The value to stakeholders will be derived from the KPI mapping with the services.

The assessment framework is graphically depicted in figure below: the green blocks are categorized as medium priority; the orange boxes are categorized as low priority and the dark blue boxes are categorized as a high priority

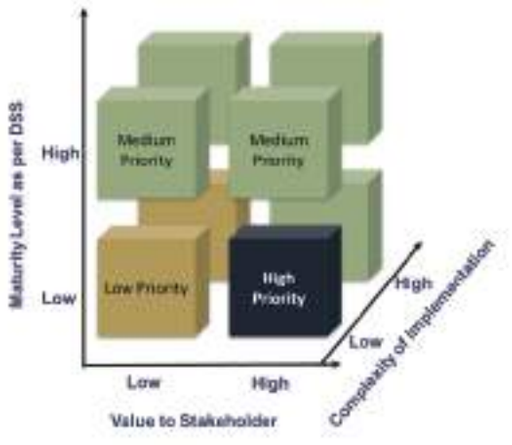


Figure 10: Service Maturity Framework

Business architecture's outcome must be a rationalized set of the service catalogue. All departments must adhere to the service catalogue and principles defined as part of the EA for Tamil Nadu.

6.5.2 *Application Architecture*

Application portfolio must be identified and catalogued under either category:

1. **State Applications**: The applications that have been deployed and customized for the state and deployed in the State Data Centre or on the cloud under the sole purview of the State Government of Tamil Nadu.
2. **Central Applications**: Developed and maintained by Government of India agencies /ministries/ divisions, this application has state specific data and support service delivery of state specific services, the services may be part of Central schemes.

Application architecture's outcome must be a rationalized set of applications portfolios along with a roadmap to enhance existing applications. All departments must adhere to principles defined as part of the EA for Tamil Nadu.

6.5.3 *Data Architecture*

The Future State representation of Data architecture comprises of following components

1. **Data Transformation**: How departments would be enabled to process data in various forms (XML, JSON, FLA File, etc.) from multiple sources.
2. **Digital Identity**: Aadhaar/GSTN could be used to create a login for the citizens/businesses. This ID would be used for access to all sector services.
3. **Data Extraction**: Extraction of data from relational databases to data warehouse for easier and efficient reporting.
4. **Data Storage**: Storage, load, and design of relational database for transactional and analytical processing.
5. **Data Analysis**: Data analysis would be enabled by both system level processing and business intelligence and data warehousing tools.
6. **Data Visualization**: All departments need tools to visualize data analysis through Business Intelligence; State-wide architecture would include such capabilities.
7. **Data Retention**: Data retention policies need to be revamped to include necessary retention requirements.
8. **Data Life-cycle Management**: Data life-cycle management would include necessary and specific requirements of the sector; however, it would be aligned to EA data life-cycle management.
9. **Data Dissemination**: Data dissemination of public data as classified in data classification model needs to be shared with the Government of India or Open Data repository.
10. **Data Authentication and Authorization**: The substantiation of the identity, definition, and enforcement of permitted capabilities of a user related to the department or system in some way.
11. **Metadata Management**: Departments participating under each sector contributing to the metadata repository are classified under their ownership.

6.5.4 *Open Data*

Another Key context for State in relation to Data Architecture is the idea of Open Data & how it should be taken up by individual departments. Open Data is the idea that a certain set of data should be freely available for everyone to use and republish as they wish. In a government context, public has the right to demand for most data using RTI (Right to Information) Act. While RTI has increased transparency, it has put tremendous workload on officers to serve these requests in a time-bound manner. Many RTI requests pertain to data that could be readily released if an Open Data policy is adopted. In other words, an effective Open Data policy implementation may mean that in addition to other benefits, the number of RTI requests on aggregate data would come down. Hence, one could see a convergence of duties between Principal Information Officers responsible for serving RTI, Data Protection Officers responsible for privacy as per the upcoming Data Protection Bill, Chief Data Officers/ Chief of Analytics responsible for Open Data policy.

1. All state entities can be driven towards releasing personally non-identifiable aggregate data under Open Data License & National Data Sharing & Accessibility Policy (NDSAP) through National platforms such as data.gov.in or equivalent in a machine readable format.
2. Open Data Policy can be developed further to ensure that RTI & data sharing goes together. Except in the case of data related to elected representatives, ideally all data that can be sought under RTI is a candidate to be put under platforms like data.gov.in

TN Data Policy 2022 has been released covering above aspects and it will give a great boost to the eco-system of value-added services that private enterprises can provide by leveraging the Government data.

6.5.5 *Value Added Services*

Enterprise Architecture team would need to ensure that the Data Architecture layer is accessible to authenticated private enterprises in a privacy compliant & secure way. Or in other words, an Open Data eco-system should be supplemented by Open-API eco-systems using which private enterprises can access Government Data, invoke business transactions or processes within the Government eco-system wherever permissible.

Once this layer is built, private enterprises & startups can leverage these APIs to develop various service centric products. Multiple eco-system partners nationally and internationally are keen to access these APIs to develop offerings at state level.

Data architecture's outcome must be a data entity description, data governance plan and data standards adherence plan. All departments must adhere to principles defined as part of the EA for TN.

6.5.6 *Technology Architecture*

The Tamil Nadu EA - Technology deployment architecture must describe the plan to assemble the assets and capabilities required for all deployments. It must define the logical and physical view of systems identified in the application architecture.

The architecture needs to provide the logical and physical component level view of the technology infrastructure. Based on the current technology details as identified, an analysis of the as-is portfolio of the technology layer has been prepared. Below are the identified Technology Solution Building Blocks for Tamil Nadu Enterprise Architecture.

- ✓ Access Devices
- ✓ Peripherals
- ✓ Network connectivity
- ✓ Network infrastructure
- ✓ Platforms
- ✓ Software Development Technology

- ✓ Computing stack
- ✓ Hosting locations

Technology architecture's outcome must be a catalogue of technology components arranged as per solution building blocks (refer to list above). All departments must adhere to principles defined as part of the EA for TN.

6.5.7 *Security Architecture*

Important steps to derive the security architecture:

1. Business and Application Need
   - ✓ Key aspects of business and application need must flow to the security architecture design
   - ✓ Key aspects of data security such as data classification must be considered
2. Assess Current State
   - ✓ A list of threats and vulnerabilities must be identified
3. Security Policy and Controls.
   - ✓ A set of policies and controls must be listed